Quick Start Guide for Azure (Windows)

Arcserve® Live Migration

Legal Notices

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified, or duplicated, in whole or in part, without the prior written consent of Arcserve. This Documentation is confidential and proprietary information of Arcserve and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and Arcserve governing your use of the Arcserve software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and Arcserve.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact Arcserve

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

https://www.arcserve.com/support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices, and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.

You can access other helpful resources appropriate for your Arcserve product.

Providing Feedback About Product Documentation:

If you have comments or questions about Arcserve product documentation, please contact us.

Contents

Chapter 1: Introduction

Arcserve Live Migration simplifies the process of migrating data, applications, and workloads. It allows you to move virtually any type of data or workload to cloud, on-premises, or remote locations, such as the edge, with support for virtual, cloud and physical systems. An assured validation of the migrated workload completes the process of enabling customers to continue operations without risks of losing data.

You can easily migrate:

From	To
On-premises	Cloud
Cloud	Cloud
Cloud	On-premises
Physical	Physical
Physical	Virtual
Virtual	Virtual

Live Migration provides the following:

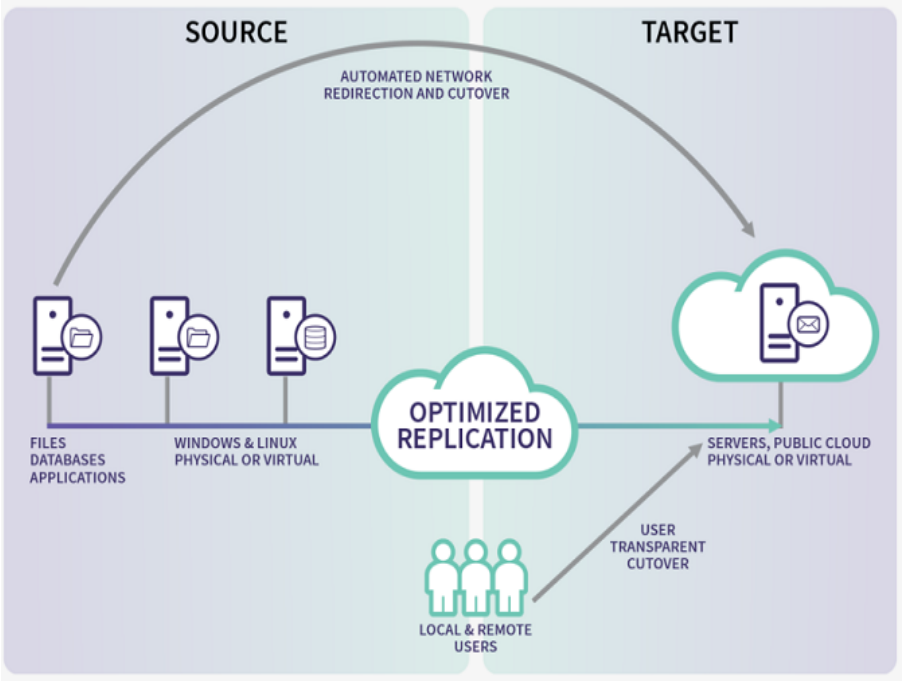
- Unlimited use of the Arcserve Live Migration technology enhanced by Arcserve Continuity Suite.
- Every source that you plan to migrate requires 1 license.
- Seamless access to the entitled software for a period of 90-days.
- On expiry of the license, new scenarios cannot be started, but the existing ones will continue.
- For each license, Live Migration provides free of cost technical assistance for two incidents.

Note: Arcserve currently does not provide professional services to help you with implementation, deployment, and any other migration services.

Overview

Arcserve Live Migration automatically synchronizes files, databases, and applications on Windows and Linux systems with a second physical or virtual environment located on-premises, at a remote location, or in the cloud. After synchronization, changes are replicated in real time to ensure the source and target are in sync prior to the migration.

Encryption enables secure data transfers between local systems and remote locations without the need for a VPN, and automated network redirection makes the switchover process seamless with push-button cutover to ensure availability to the new production environment.



Your typical migration process includes the following steps:

- Install Components on Master
- Configure Microsoft Azure
- Provision Virtual Appliance (VA) on Azure
- Install Engine on Replica
- Create Full System Scenario for Microsoft Azure
- Perform Assured Recovery Testing
- Perform Cut off/Switchover

Terminologies

This document uses the following terminologies:

- **Virtual Appliance:** This is a virtual machine that acts as the Replication/Migration proxy server (install the Arcserve Continuity Suite Engine here and deploy on the hypervisor/cloud destination). If you are using a Hyper-V virtual platform, the Virtual Platform Hostname/IP field is disabled (appears dim).
- **Control Service:** Control Service is a management component of Arcserve Continuity Suite. It is a Windows based service that must be deployed first. It hosts web-based information portal and rich Management UI, which is used for creating and monitoring migration scenarios.
- **Engine:** Replication Engine is a background service that moves data from source to destination during migration. Install the Engine on any source that you plan to migrate. You may use the Remote Installer feature to mass deploy Engines.
- **FSHA:** Full System High Availability (FSHA) is a scenario type that allows replication and fail-over of full server. This scenario type is used for migrating full systems.
- **Management UI:** A UI that you use for creating and managing replication/migration scenarios. The Control Server hosts the Management UI. To start the Management UI, log into the Management Portal.
- **Master (Source):** A host/computer that you want to migrate. You can migrate the whole system using the full system migration scenario or the host containing the applications.
- **PowerShell:** Arcserve offers PowerShell Command Line Interface as an alternative if you do not want to manage the replication process using the Manager graphic user interface.
- **Replica (Target):** In case of full system migration, VA (replication proxy) serves as a Replica. Upon completion, VA spins off new VM containing replicated disks or data. For application-based scenarios, the VA hosts and runs replicated application and data.
- **Scenario:** A configuration unit describing migration job/task. You can create and manage scenarios using rich management GUI or PowerShell CLI. Scenarios contain key information about replication/migration jobs to be performed.

- **Switchover:** The cutover to the newly migrated workload from where the operations can begin.
- **Synchronization:** The process of making the set of files identical on the Master and Replica servers. It is usually necessary to synchronize the Master and Replica as the initial step of a replication/migration scenario.
- **Virtual Platform Host:** The machine that hosts the Appliance VM, which acts as a Replica server. Based on the scenario type, it acts as a local hypervisor or cloud platform (AWS or Azure).

Requirements

Before you migrate, make sure to meet the following requirements:

- Arcserve Live Migration supports both Windows and Linux operating systems for Full System migration scenarios. If source host is Windows, then the Virtual Appliance (VA) must be Windows; if source host is Linux, then the VA must be Linux as well.

  Note: Before deploying Arcserve Live Migration scenarios, see Limitations in Release Notes.

- When migrating workloads to Azure, corresponding Azure cloud credentials must be registered in Arcserve Continuity Suite Management UI.

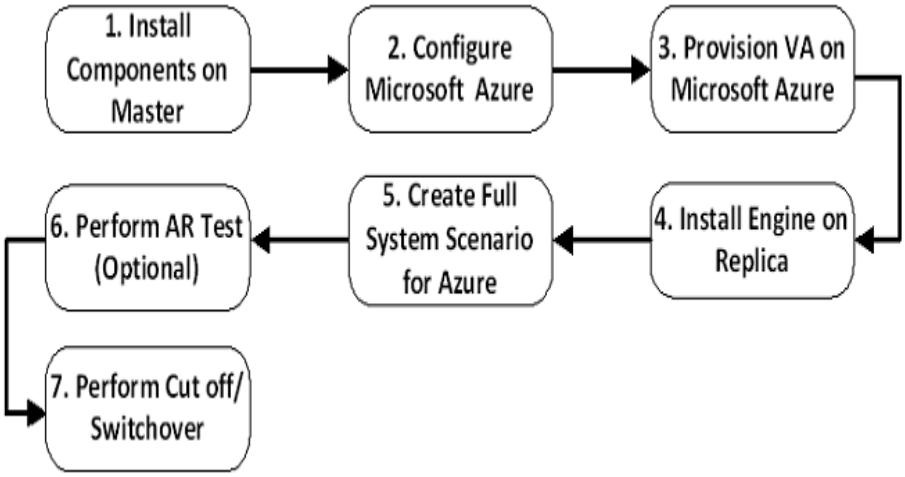
Software Compatibility

For more information about compatibility, see the Compatibility Matrix.

Note: Make sure that your source OS and application versions are explicitly listed on support matrix.

Chapter 2: Perform Live Migration

The following flowchart provides the Live Migration process given in this document:



Install Components on Master

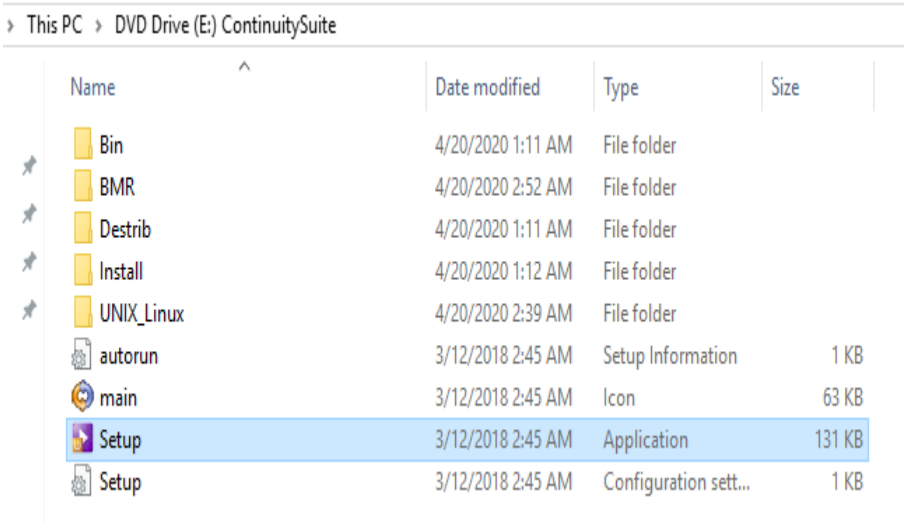
This section describes how to install the Arcserve Continuity Suite Control Service and Engine on Master.

Installing Control Service

The Control Service component functions as the single-point-of-control that contains the entire dataset of the existing scenarios. Control Service communicates with the Engines and the Managers. It is responsible for the management of all scenario-related-tasks, such as creation, configuration, monitoring, and running of the scenarios.

To install Control Service, follow these steps:

1. Download RHA iso for Continuity Suite, and then open the folder.
2. From the mounted directory, double-click **Setup**.

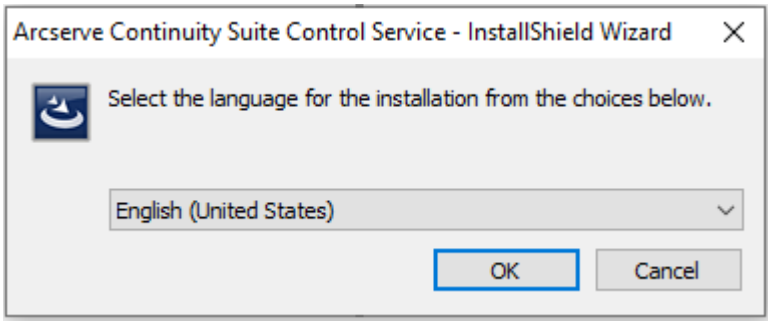


3. On the Arcserve Continuity Suite installation wizard, click **Install Components**.

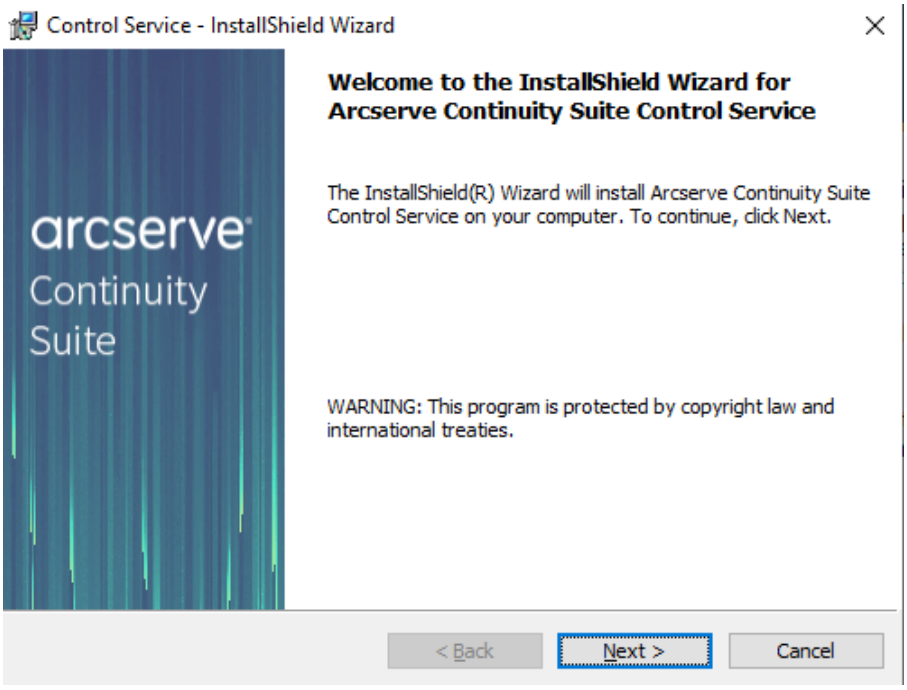
The wizard displays the components.

4. Click **Install Control Service**.

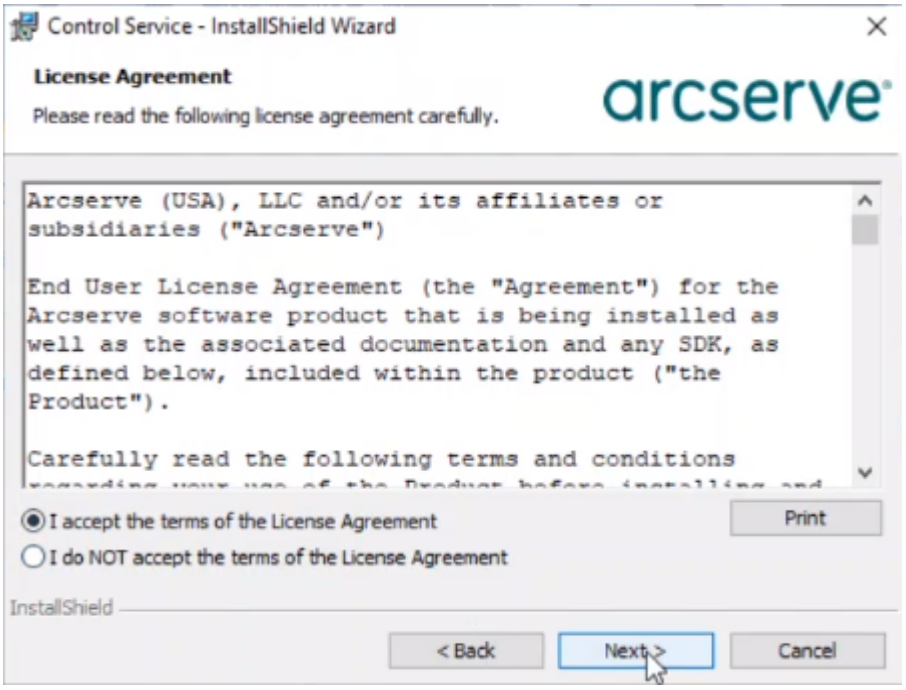
5. On the Arcserve Continuity Suite Control Service - InstallShield Wizard, from the drop-down list, select your preferred language, and then click **OK**.



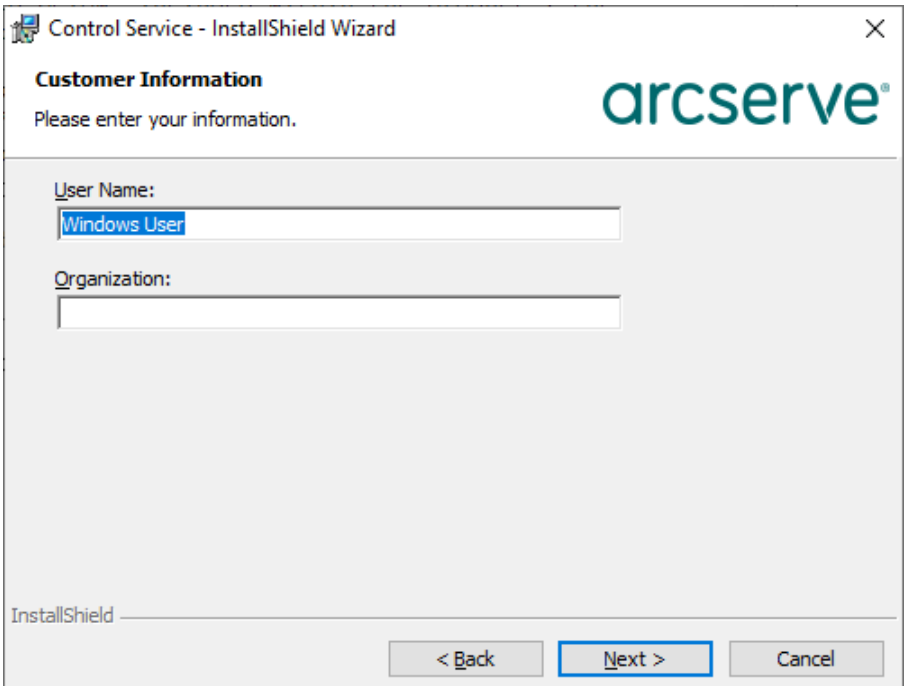
After the initial process is complete, the Welcome page appears.



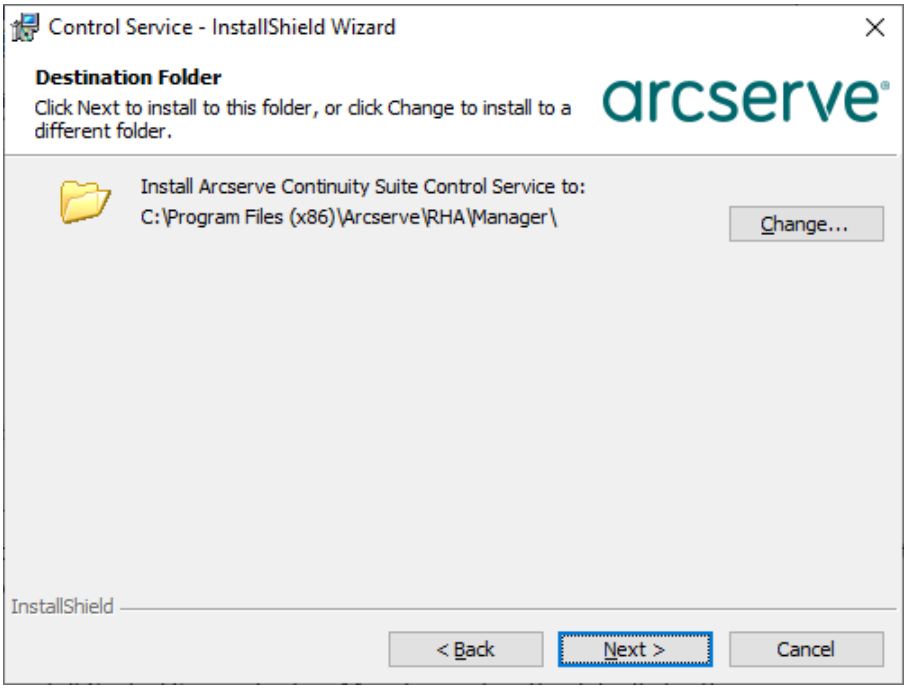
6. Click **Next**.
7. On the License Agreement page, read the terms of the License Agreement, select the **I accept the terms of the License Agreement** option, and then click **Next**.



8. On the Customer Information page, enter a user name, and then click **Next**.



9. On the Destination Folder page, retain the defaults, and then click **Next**. To change the destination folder, click **Change**.

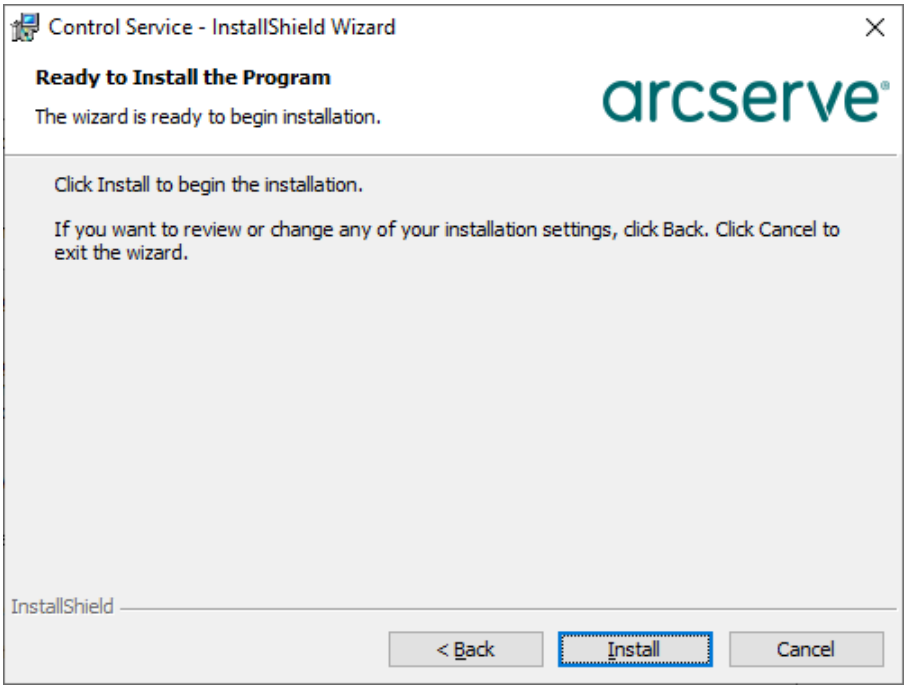


Note: The default installation directory is: *C:\Program Files (x86)\Arcserve\RHA\Manager*. All executables, DLLs and configuration files are located within the INSTALLDIR.

10. For the upcoming screens, retain the defaults, and then click **Next** to continue.

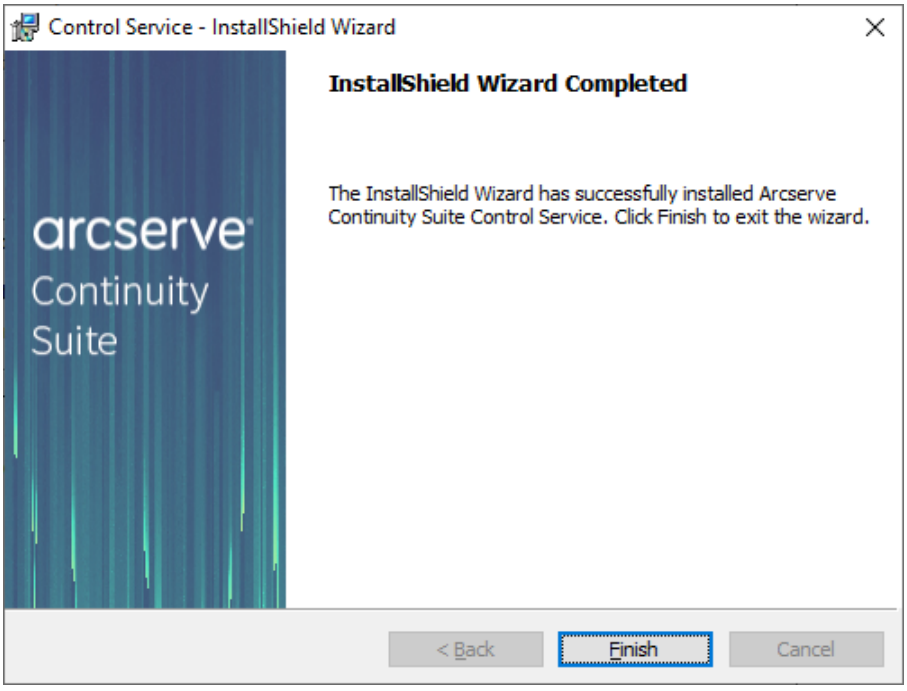
    Note: For more information about how to configure SSL Configuration, Service Logon Information, and Control Service Role, see Install a Control Service for a Standard Operation.

11. On the Ready to Install the Program page, click **Install**.



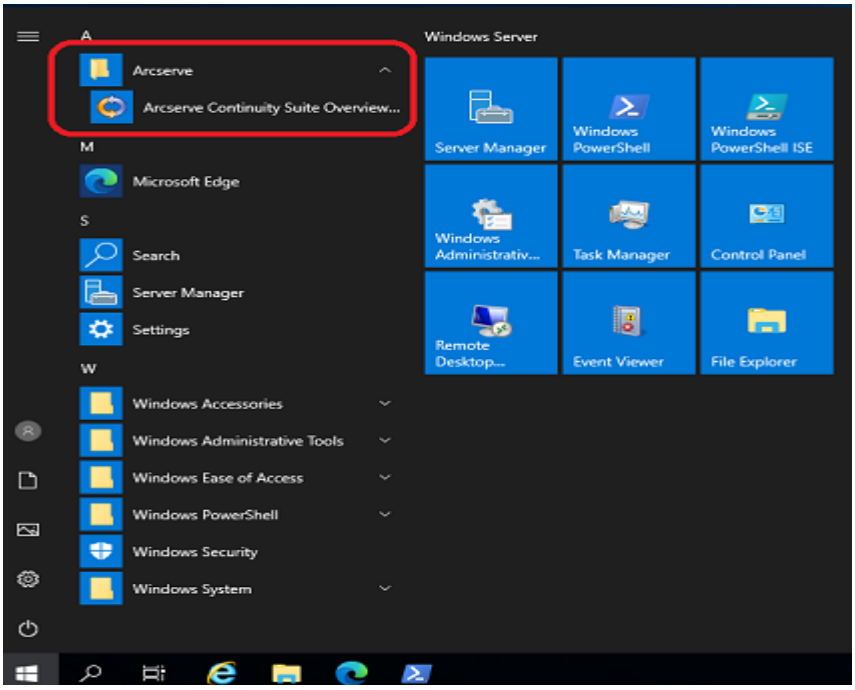
Note: Click the **Back** button to return to the previous pages and change any configuration as needed.

12. After installation is complete, click **Finish** to close the wizard.

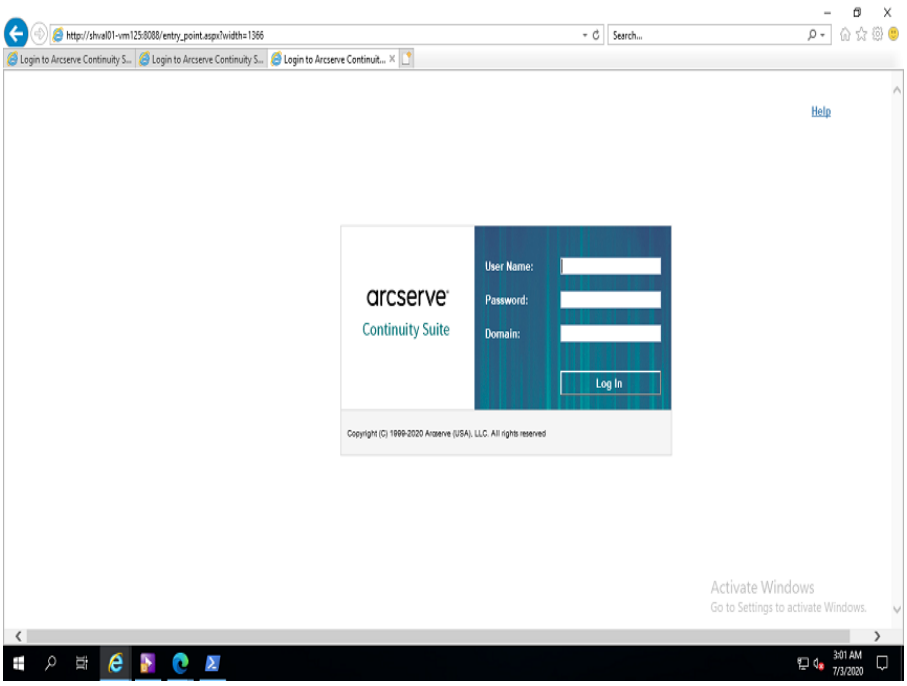


The Arcserve Continuity Suite Control Service is installed.

13. To open Control Service in a web portal, go to **Start** > **Arcserve** > **Arcserve Continuity Suite Overview**.



The web portal opens in a browser.

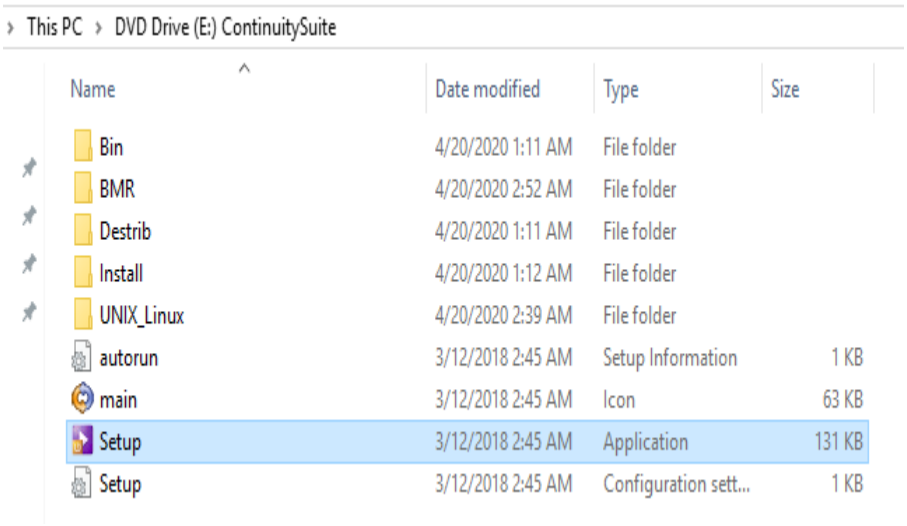


Installing Engine

Make sure that the Engine component, which is a service, is running before you start any scenario. Install Engine on every server participating in any given scenario such as the Master (source) and Replica (target) hosts. Each Engine supports both Master and Replica functionality in addition to both Replication and High Availability scenarios. It may participate in multiple scenarios and serve in a different role for each scenario. You can install Engines one by one locally on each host, or concurrently through a remote installer on numerous hosts. You can also install it during scenario creation if needed.

To Install Engine, follow these steps:

1. Download RHA iso for Continuity Suite, and then open the folder.
2. Open the Continuity Suite mounted directory, and then double-click **Setup**.

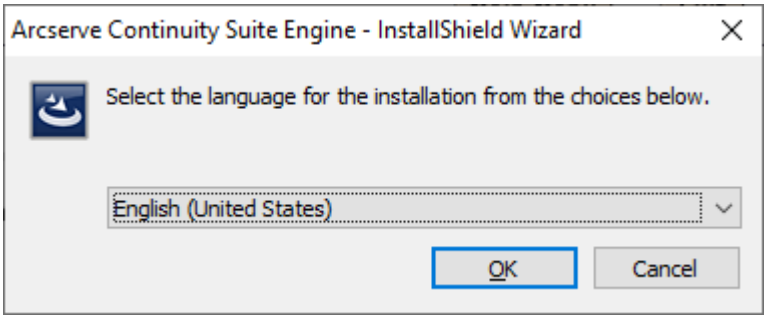


3. On the Arcserve Continuity Suite installation wizard, click **Install Components**.

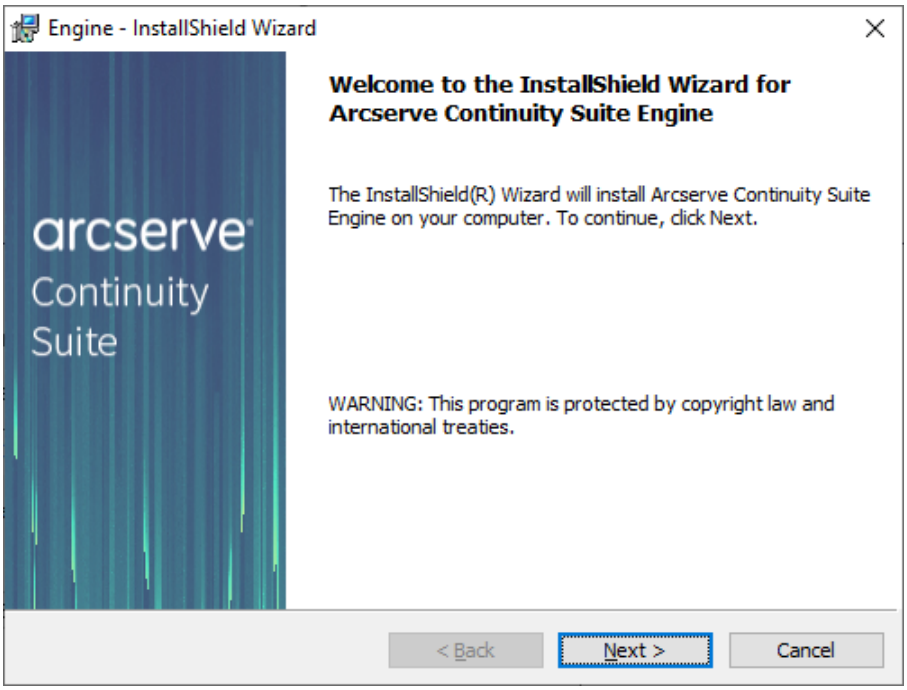
The wizard displays the components.

4. Click **Install Engine**.

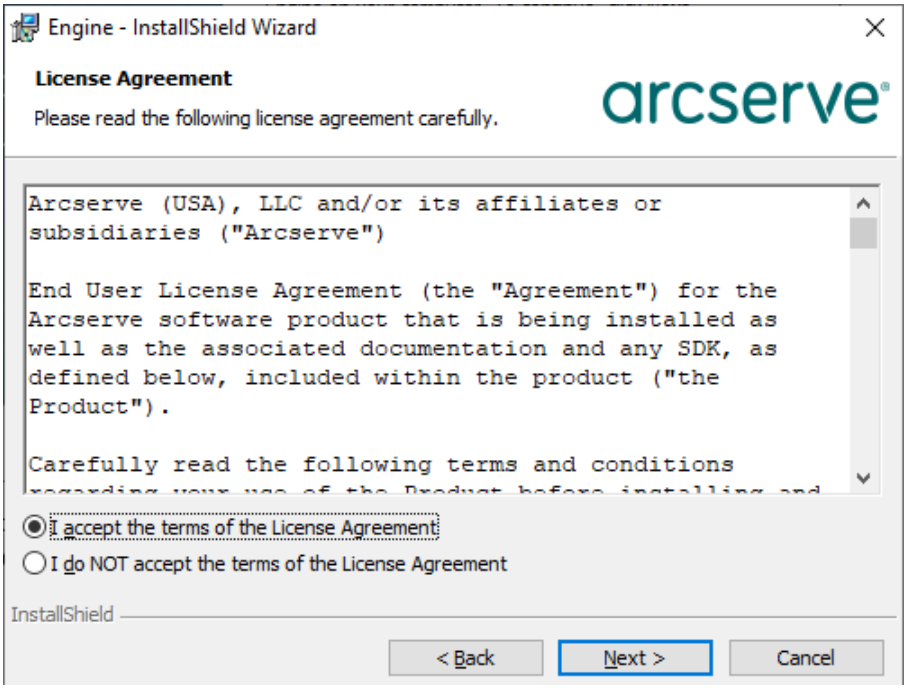
5. On the Arcserve Continuity Suite Engine - InstallShield Wizard, from the drop-down list, select your preferred language, and then click **OK**.



After the initial process is complete, the Welcome page appears.

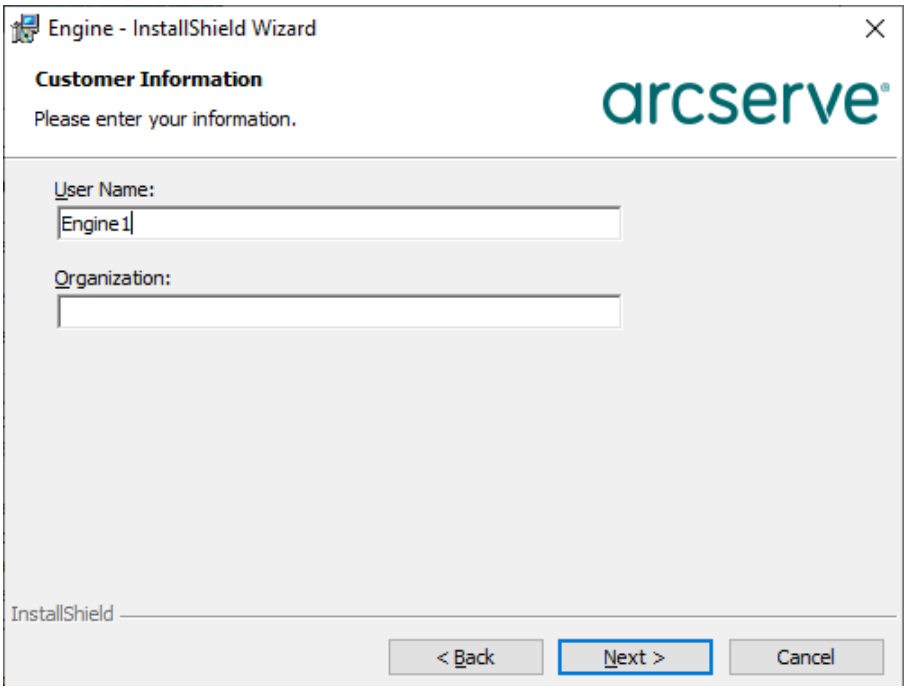


6. Click **Next**.
7. On the License Agreement page, read the terms of the License Agreement, select the **I accept the terms of the License Agreement** option, and then click **Next**.

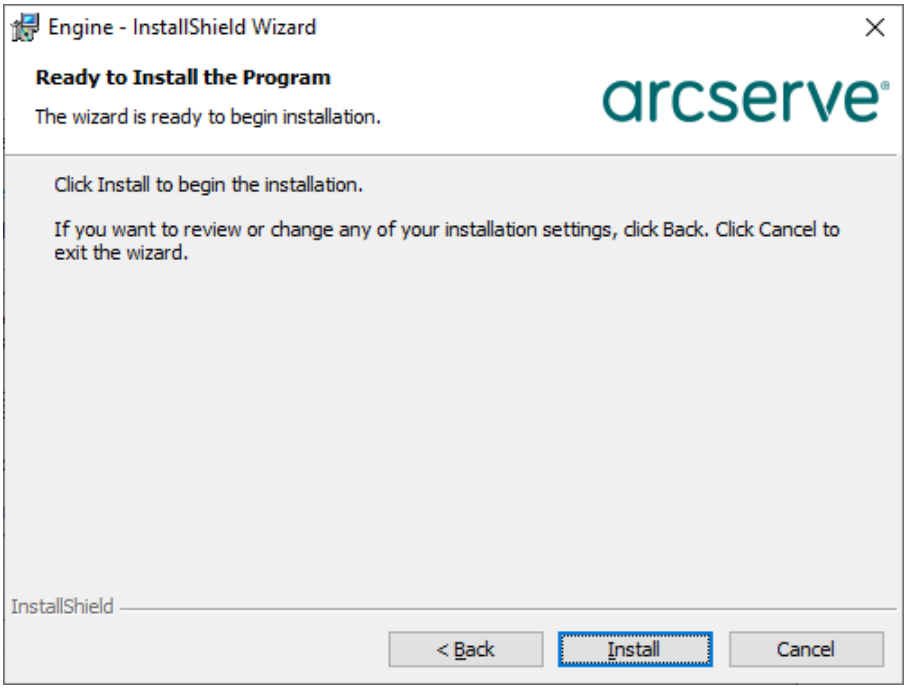


Note: If an Engine from the previous version exists on your server, the information about the previous version page appears with an option to uninstall the Engine.

8. On the Customer Information page, enter a user name, and then click **Next**.

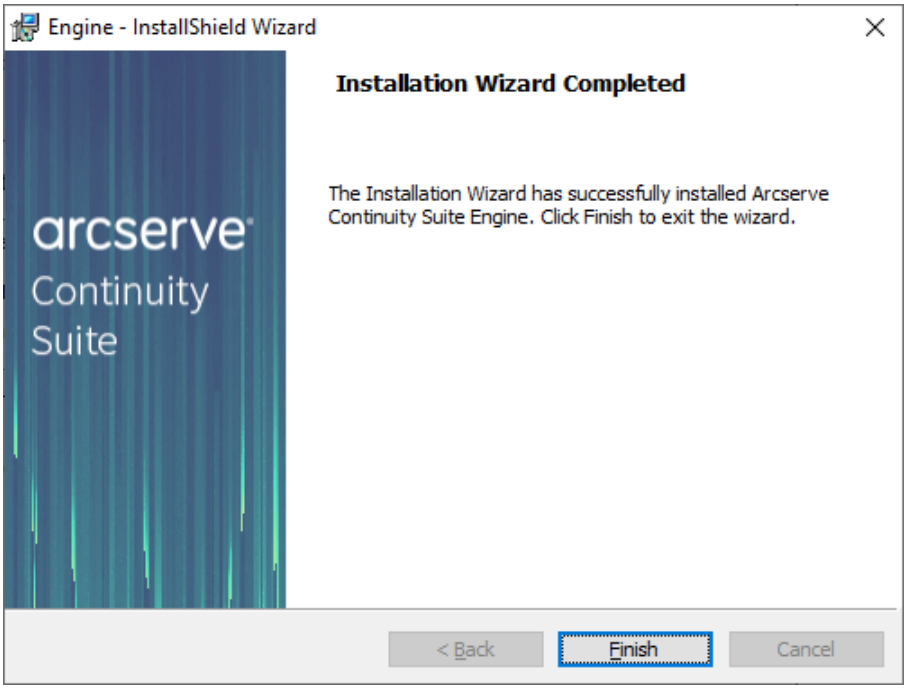


9. For the upcoming screens, retain the defaults, and then click **Next** to continue.
10. On the Ready to Install the Program page, click **Install**.



Note: Click the **Back** button to return to the previous pages and change any configuration as needed.

11. After installation is complete, click **Finish** to close the wizard.



The Arcserve Continuity Suite Engine is installed.

Configure Microsoft Azure

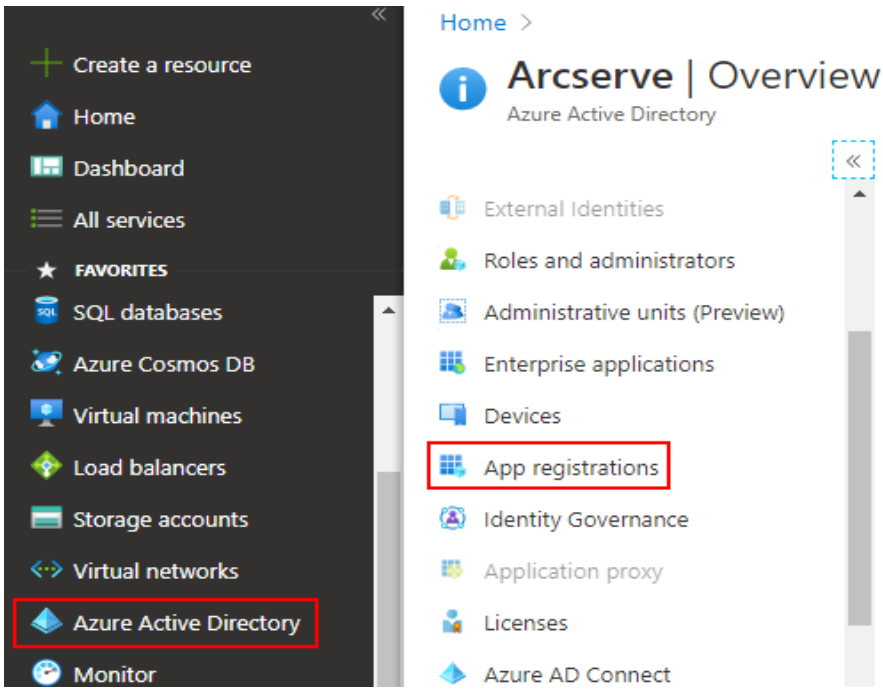
Arcserve Replication and High Availability needs some of the Azure properties for the Full System scenario to work with Azure. Before adding an account in the Continuity Suite manager, you need to configure Microsoft Azure, which includes generating the following account information:

- E-mail Address
- Subscription ID
- Tenant ID (Directory ID)
- Application ID
- Client Key

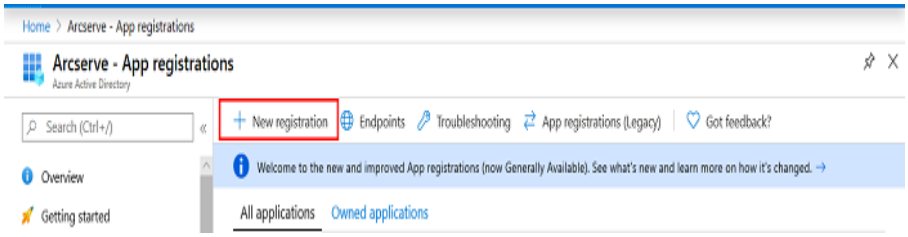
First, prepare the Azure cloud account, and then add the account in Continuity Suite Manager.

To configure an Azure Cloud account, follow these steps:

1. Perform the following steps to register an Azure Active Directory application:
   a. Log into the Azure portal.
   b. From the left pane, select **Azure Active Directory**, and then click **App registrations**.

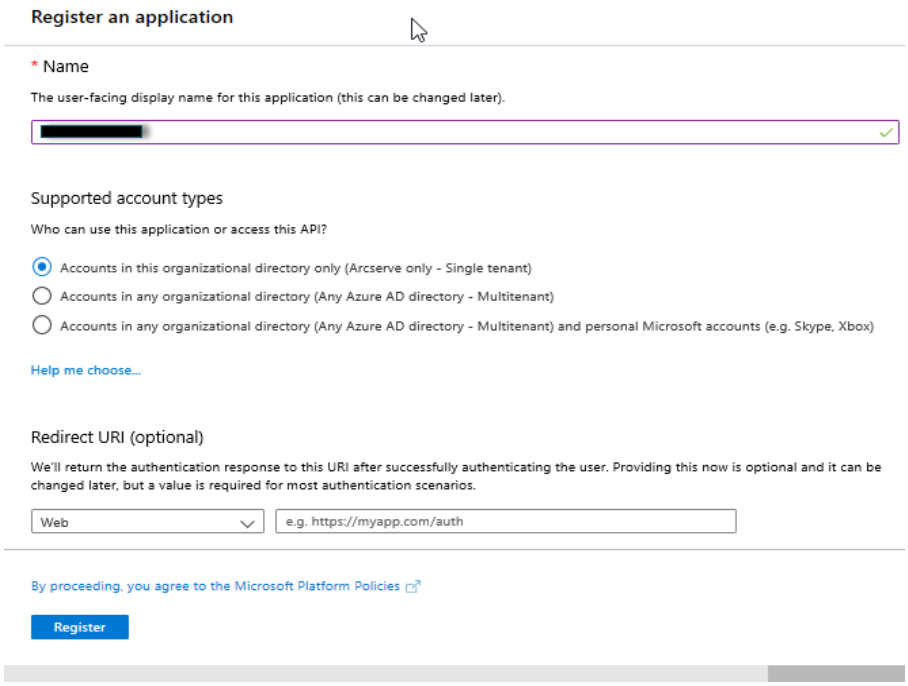


   c. On the Arcserve- App registrations page, click **New registration**.

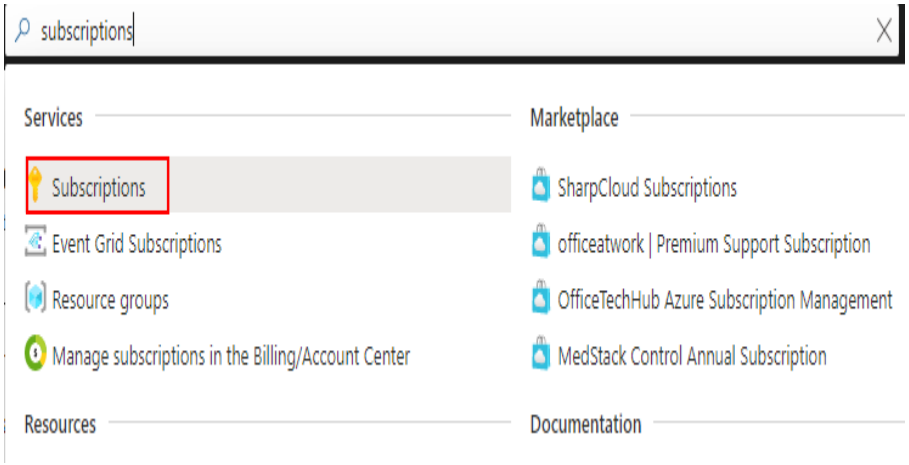


d. On the Register an application page, do the following, and then click **Register**:

- Name - Enter a name for the application.
- Supported account types - Select a supported account type, which determines who can use the application.
- Redirect URI (optional) - Select **Web or Public client (mobile & desktop)** for the type of application you are creating, and then enter the redirect URI for your application.



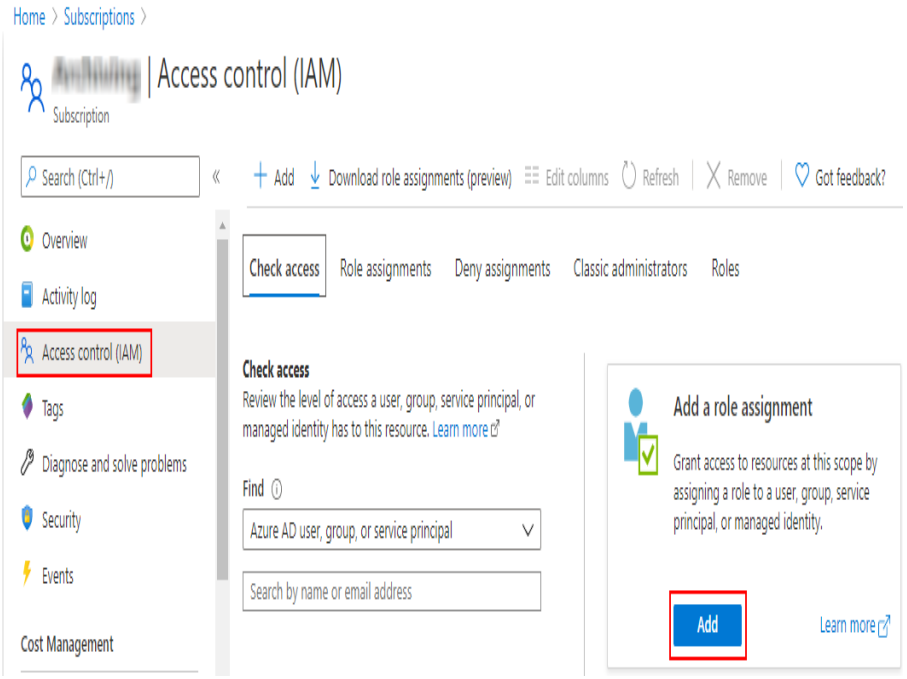
e. On the search bar, type subscriptions, and then from the list, click **Subscriptions**.



f. On the Subscriptions pages, select the subscription for your application.

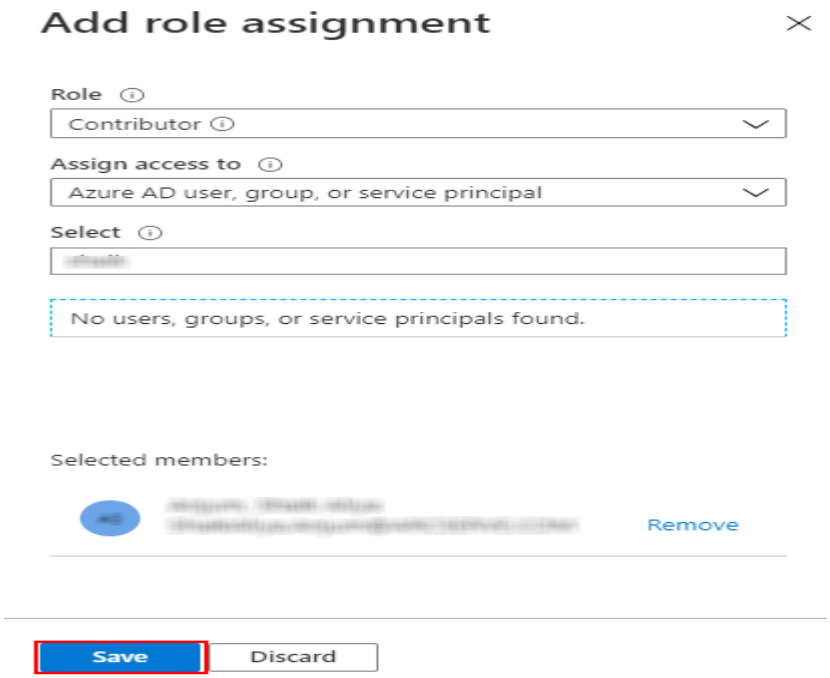
Note: If the subscription list does not display the required subscription, select **global subscriptions filter**. Make sure the subscription you want is selected for the portal.

g. From Subscriptions, go to **Access control (IAM) > Check access**, and the click **Add** from the Add a role assignment box.



h. On the Add role assignment page, do the following, and then click **Save**:

- Role - Select the role you want to assign to the application.
- Assign access to - Leave it as default.
- Select - By default, the Azure AD applications do not display in the available options. To find your application, search for the name, and then select it.

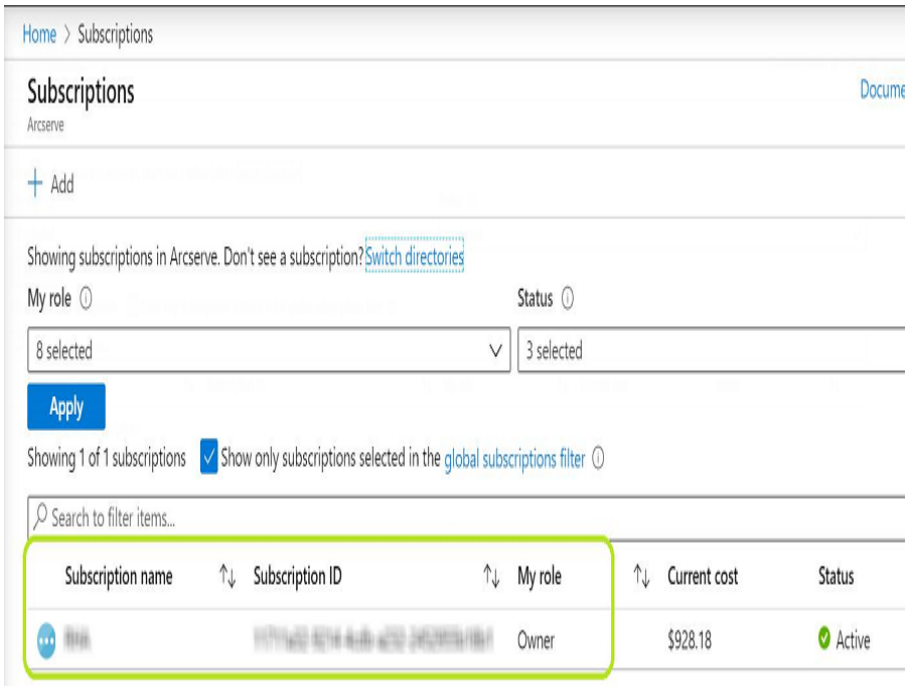


The Azure Active Directory application is registered, and a role has been assigned to it successfully.

Now, you can perform the next steps using the registered application to get the required IDs and Key.

2. To get the Subscription ID[1], follow these steps:
   a. From the left navigation pane of Azure portal, click **Subscriptions**.

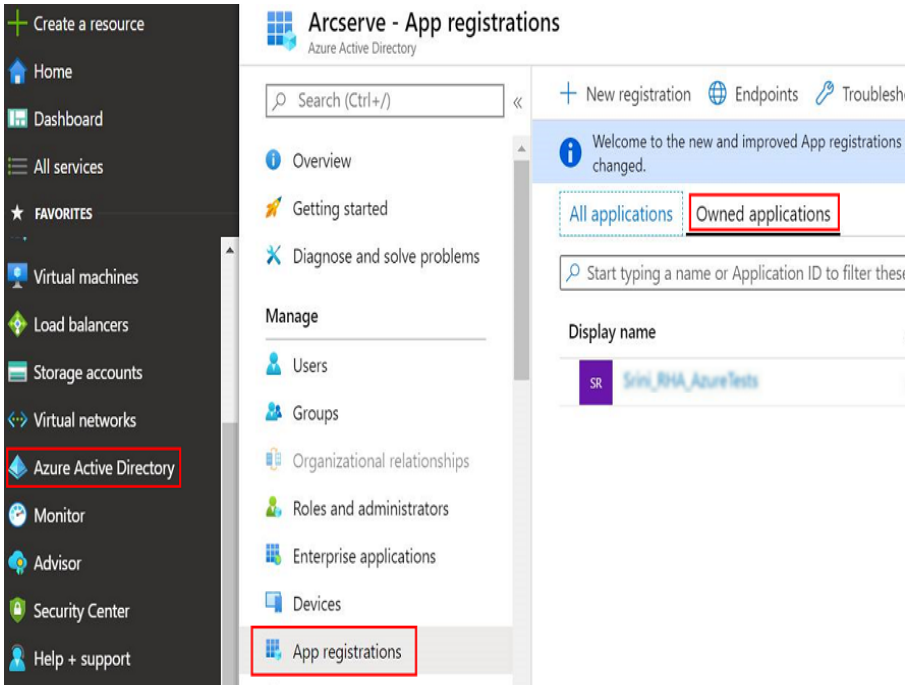
      The list of your subscriptions is displayed along with the subscription ID.



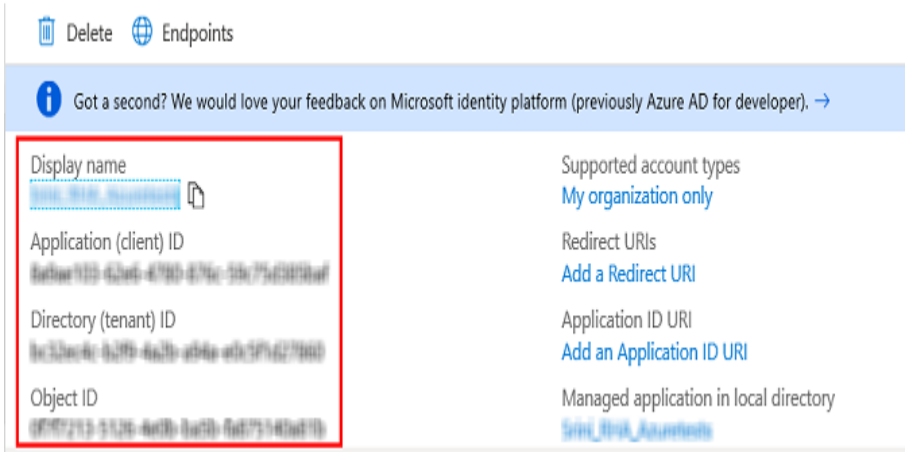
   b. Copy the subscription ID, which is used while adding the account in Continuity Suite Manager.

3. To get the Tenant ID[2] and Application ID[3], follow these steps:
   a. Navigate to **Azure Active Directory** > **App registrations** > **Owned applications**, and then select your application.

[1]The Subscription ID refers to a GUID (Globally Unique Identifier) that uniquely identifies your subscription to use Azure services.
[2]Tenant ID refers to the ID of the Azure Active Directory where you created the application registration. Tenant ID is called Directory ID inside Azure Active Directory Properties.
[3]An Application ID refers to a GUID that uniquely identifies the app's registration in the Azure Active Directory tenant. Sometimes, it is also referred as Client ID.



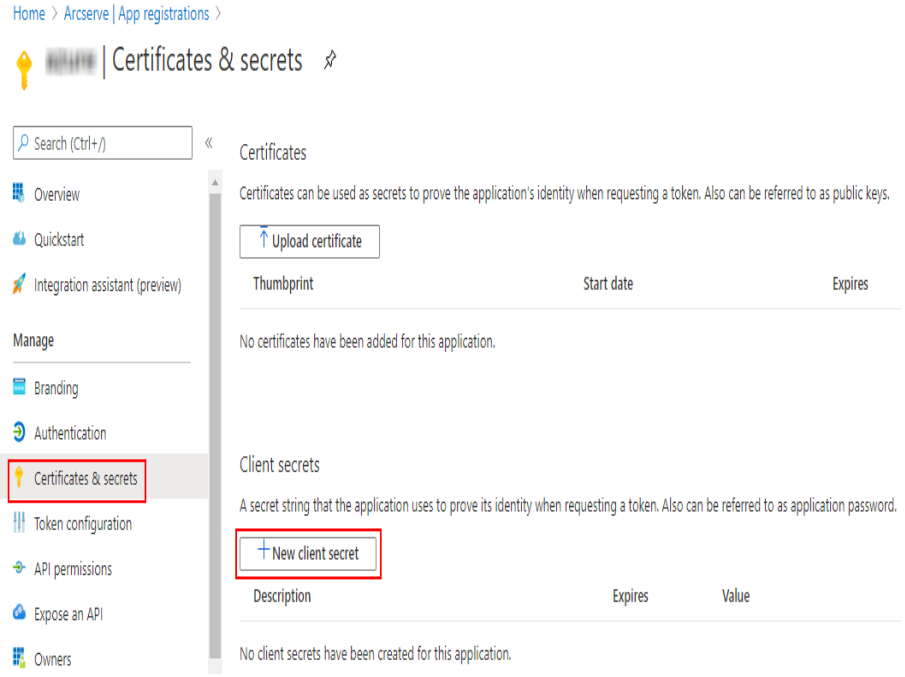
b. Copy the Tenant ID and Application ID, which are used while adding the account in the Continuity Suite Manager.



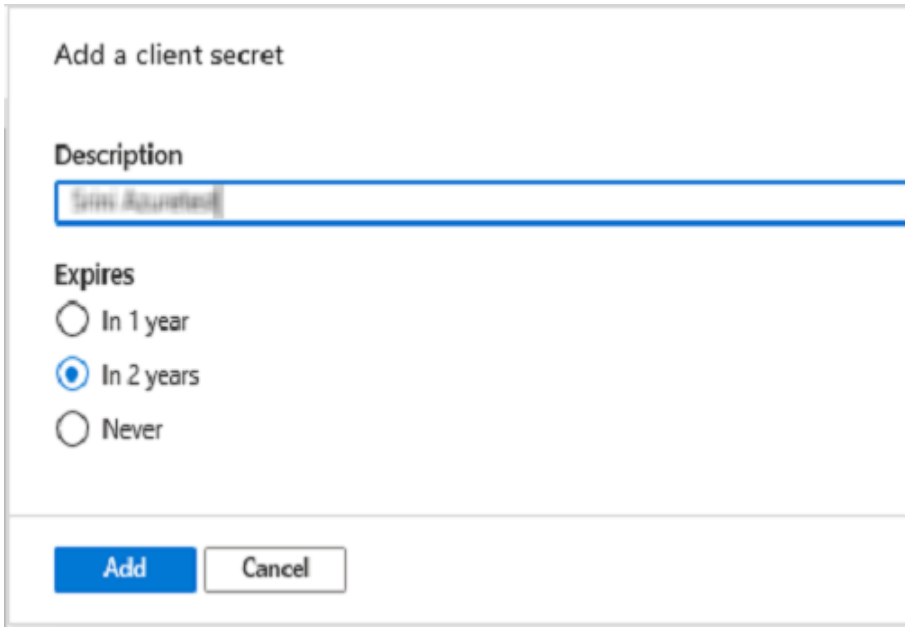
4. To get the Client secret[1], follow these steps:

   a. On the App registrations page, select the application, navigate to **Certificates & secrets** on the left pane, and then click **New client secret** to add a client secret.

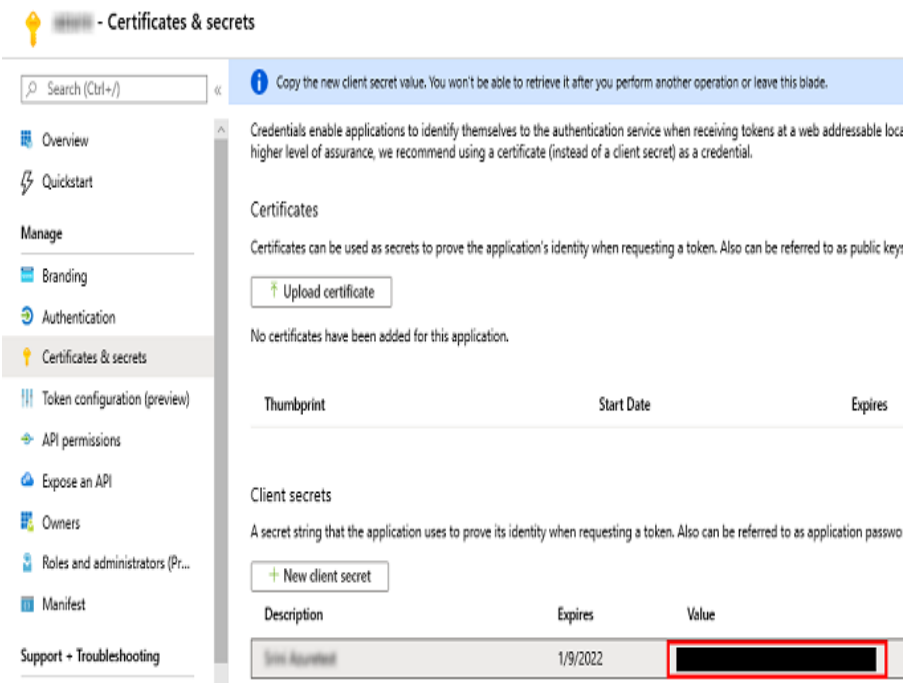
[1]Client secret is referred as an authentication key in Azure.



b. On the Add a client secret page, enter the description, select the expiry interval, and then click **Add**.



The client secret value is displayed.



Important! Copy and save this value as you cannot retrieve it later.

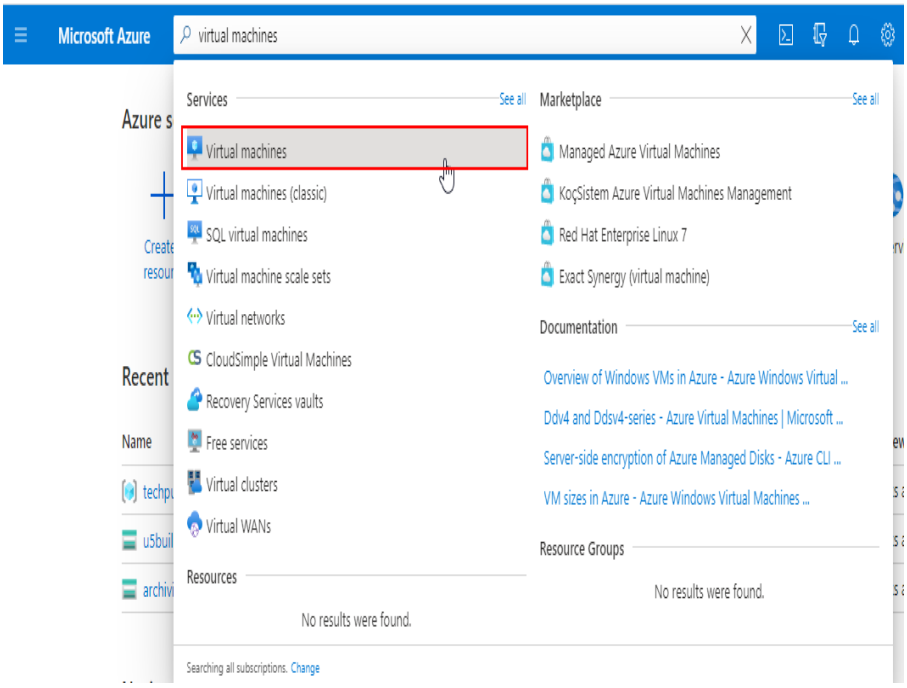
The Azure account for Live Migration is now configured.

Provision VA on Microsoft Azure

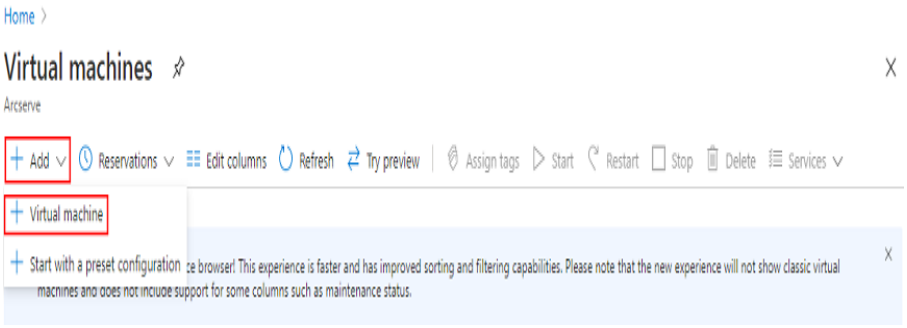
The Continuity Suite Virtual Appliance (VA) is a VM running on the virtualization platform or cloud where you want to replicate the Master servers. The VA acts as Replica in a Continuity Suite Full System scenario. The Master server is replicated to this virtualization platform or cloud. However, the Disaster Recovery VM of Master server starts and runs on this virtualization platform or cloud for multiple reasons, such as Assured Recovery testing, Switchover, and Start VM.

Follow these steps:

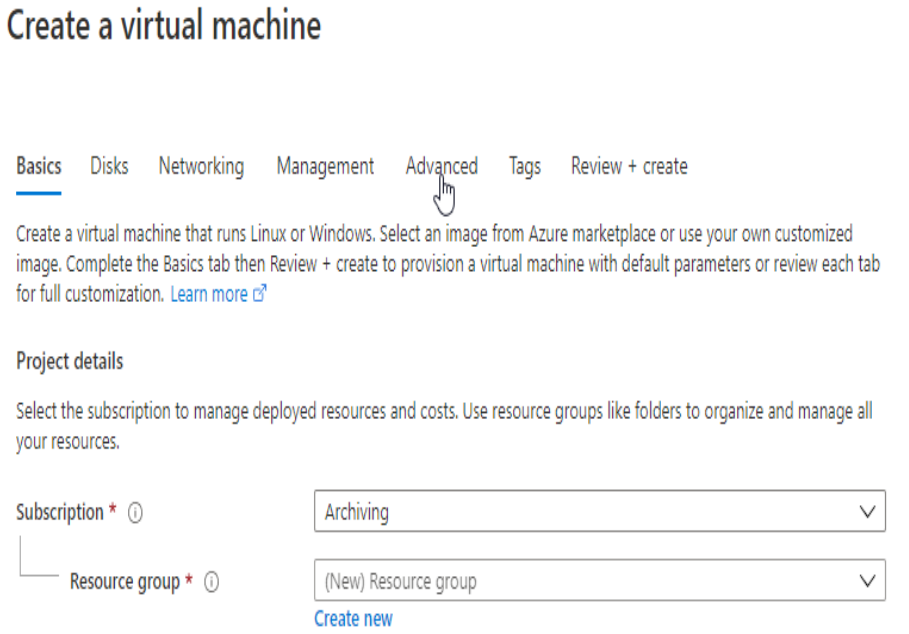
1. Log into the Azure Portal.
2. Search for virtual machines in the search bar, and then select **Virtual machines**.



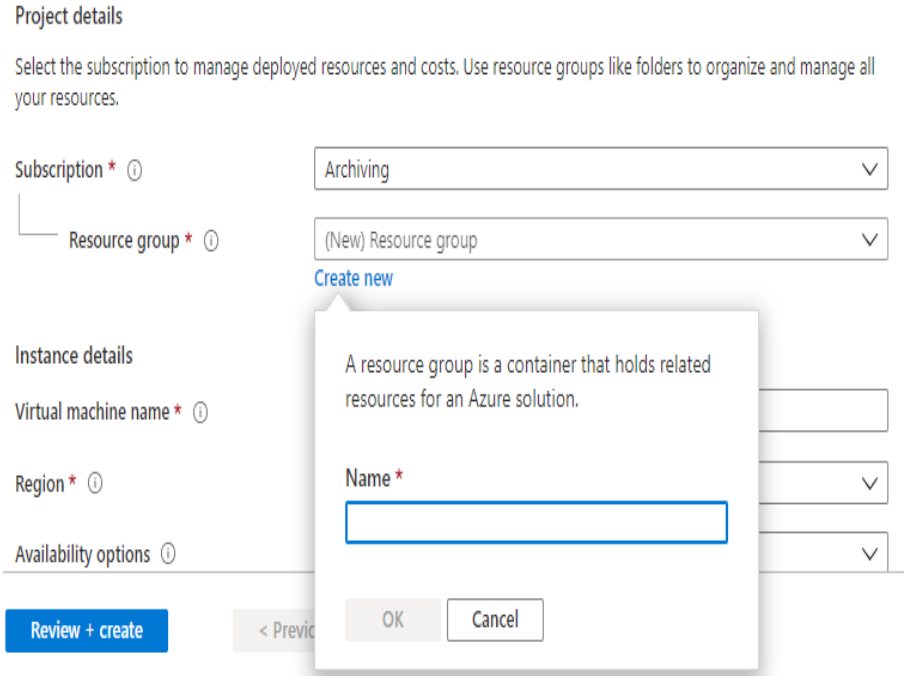
3. On the Virtual machines page, click **Add**, and then click **Virtual machine**.



The Create a virtual machine page appears.

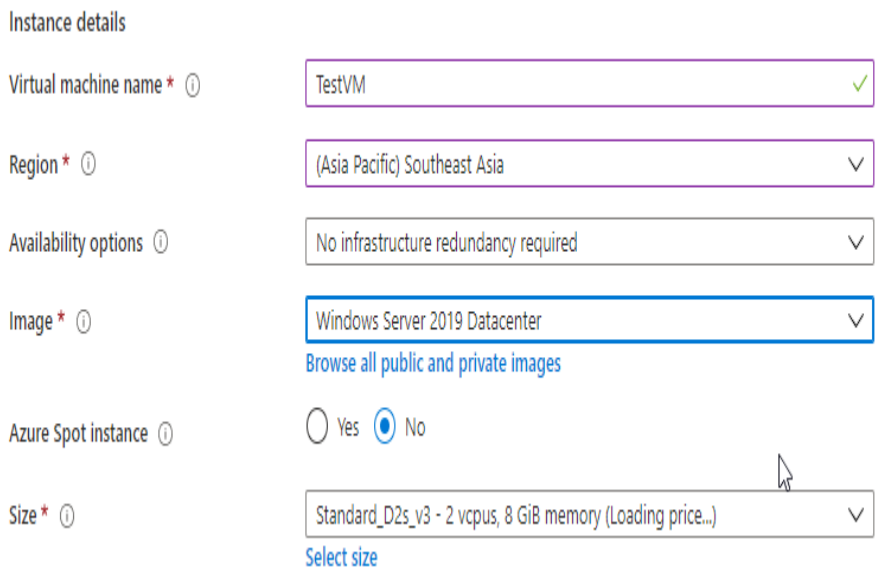


4. On the Basics tab, under Project details, do the following:
   - Subscription - Select the correct subscription.
   - Resource group - Select the existed resource group from the drop-down list or click **Create new** to create a new resource group. Enter a name for the resource group, and then click **OK**.



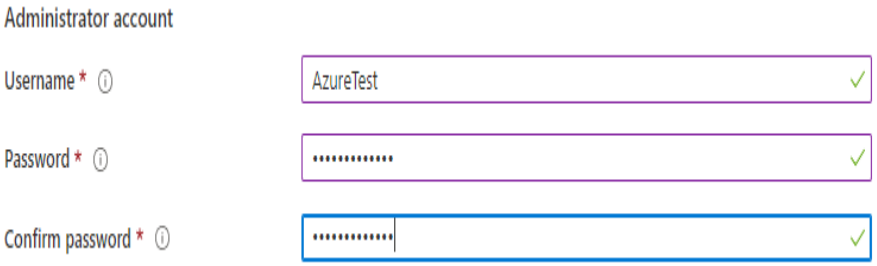
5. Under Instance details, do the following, and retain defaults for the rest:

- Virtual machine name - Enter a name for the virtual machine.
- Region - Select the required region.
- Image - Select the required image.

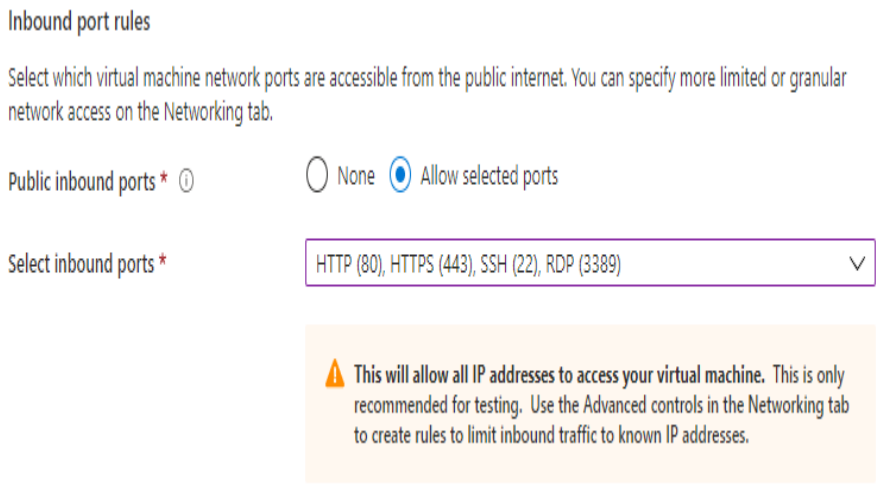


6. Under Administrator account, provide a user name and password.

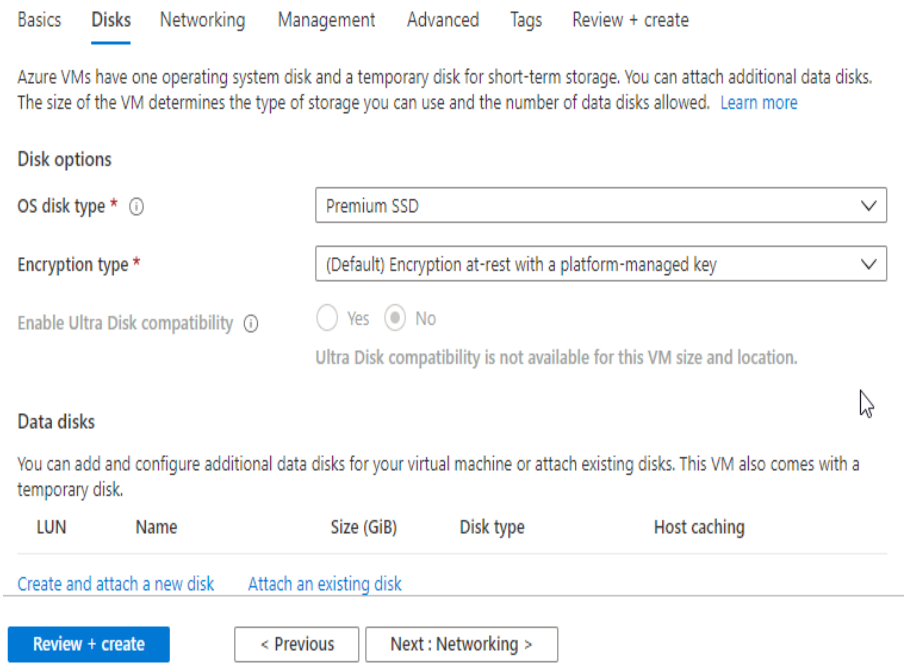
   Note: The password must be at least 12 characters long and meet the defined complexity requirements.



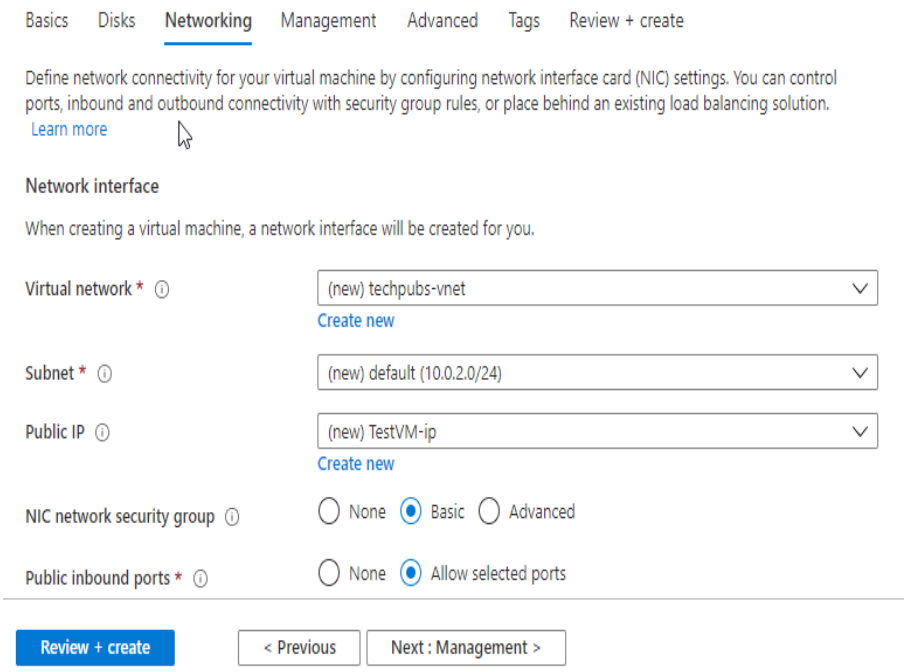
7. Under Inbound port rules, do the following:
   - Public inbound ports - Select **Allow selected ports**.
   - Select inbound ports - From the drop-down list, select all the inbound ports so that all the ports get enabled when you use this option.



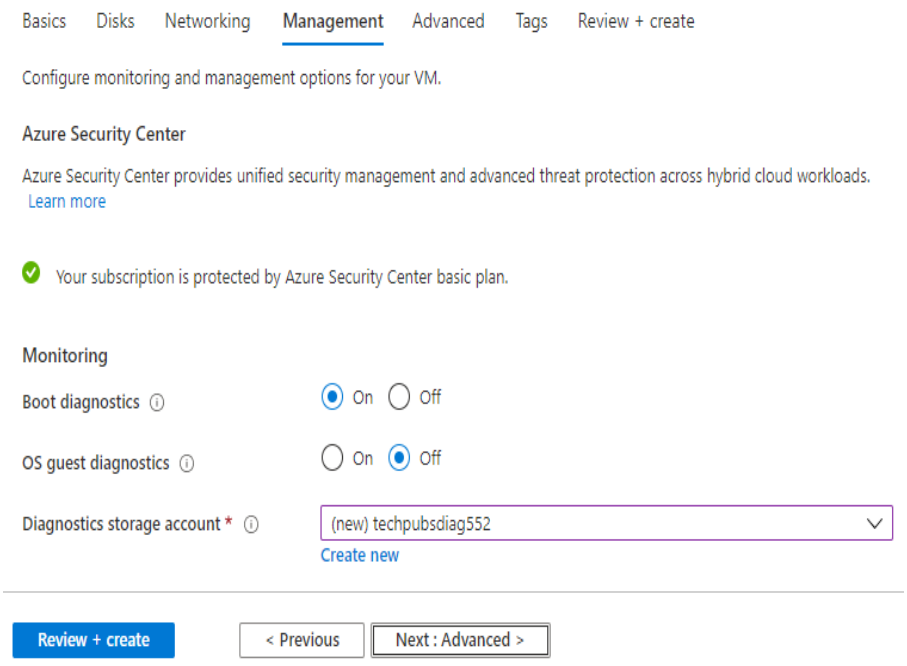
8. Retain defaults for the rest, and then click **Next: Disks**.
9. On the Disks tab, we recommend using the default settings, however you may make changes as needed. Click **Next: Networking**.



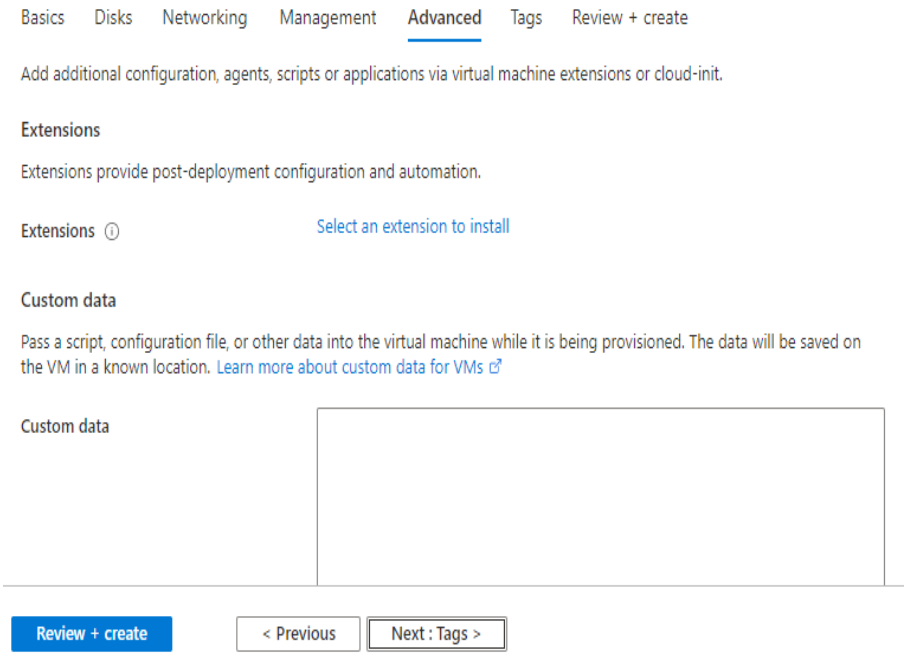
10. On the Networking tab, we recommend using the default settings, however you may make changes as needed, and then click **Next: Management**.



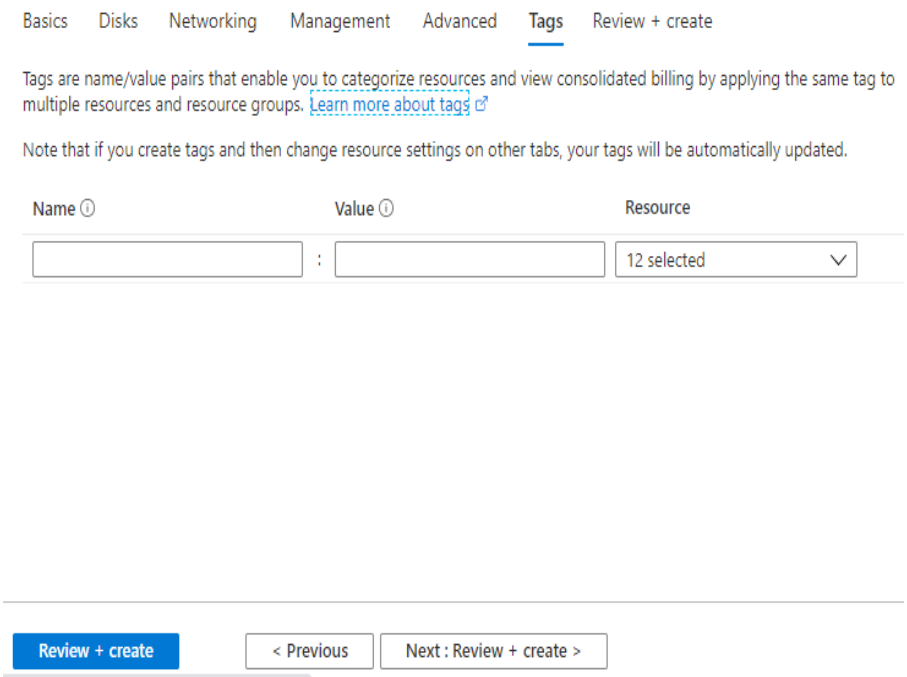
11. On the Management tab, we recommend using the default settings, however you may make changes as needed, and then click **Next: Advanced**.



12. On the Advanced tab, click **Next: Tags**.

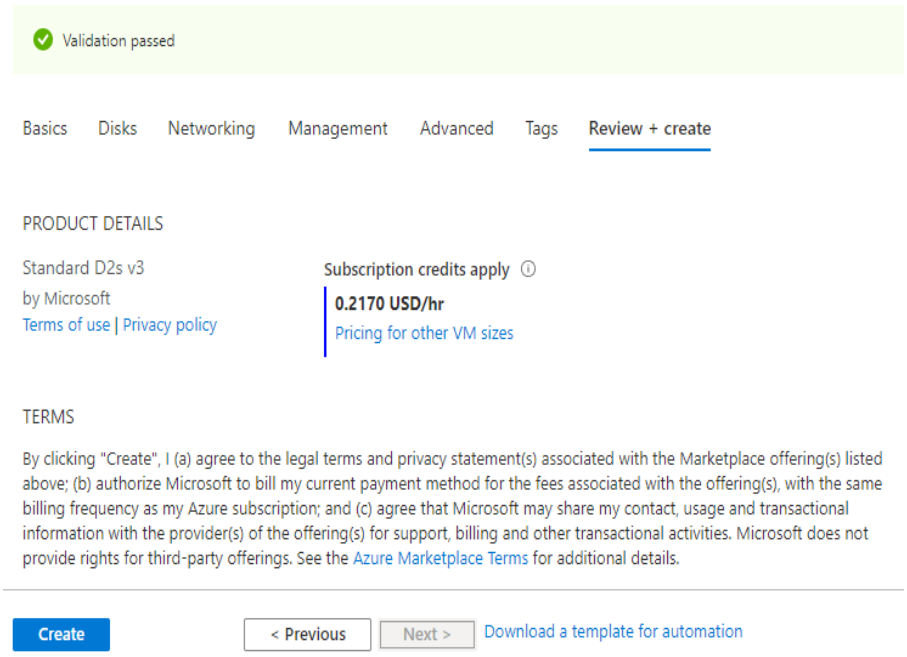


13. On the Tags tab, click **Next: Review + create**.



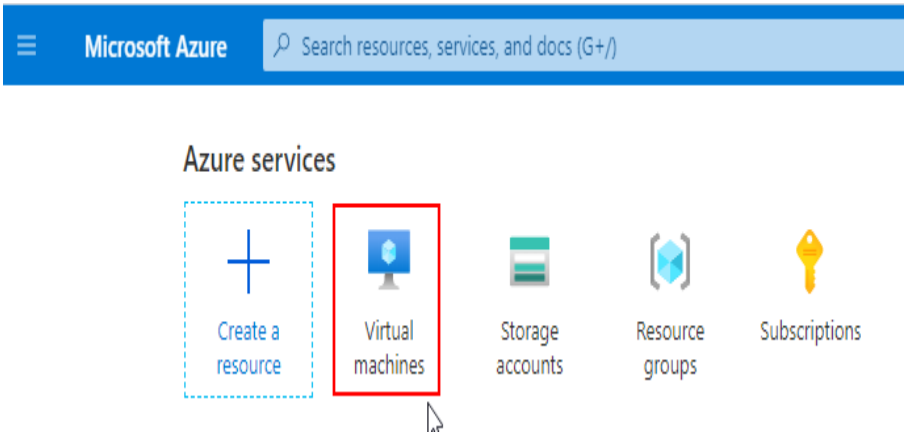
On the Review + create page, the *Validation passed* message appears.

14. On the Review + create tab, click **Create**.

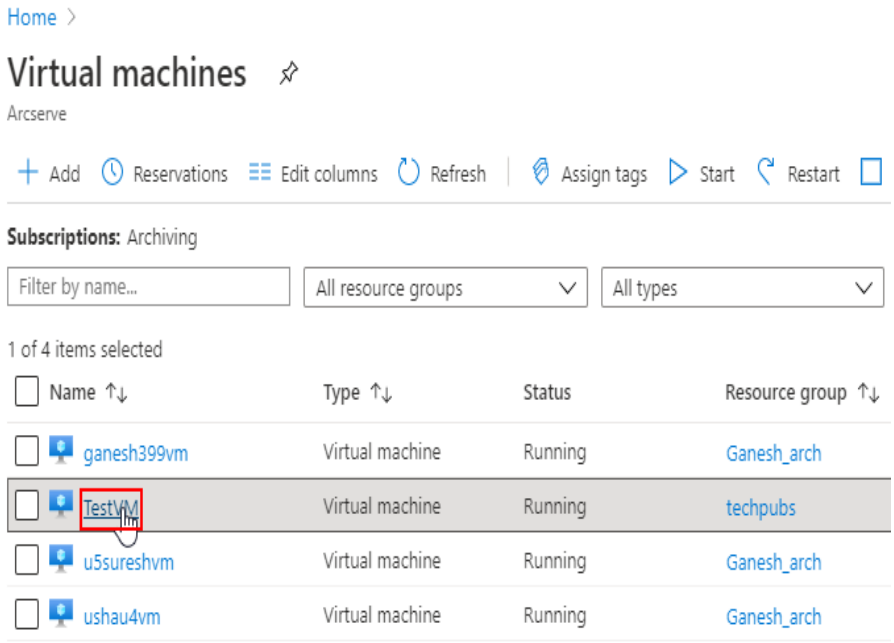


Wait until the deployment process is complete.

15. Navigate to Home tab on the top-right corner, and then click **Virtual machines**.

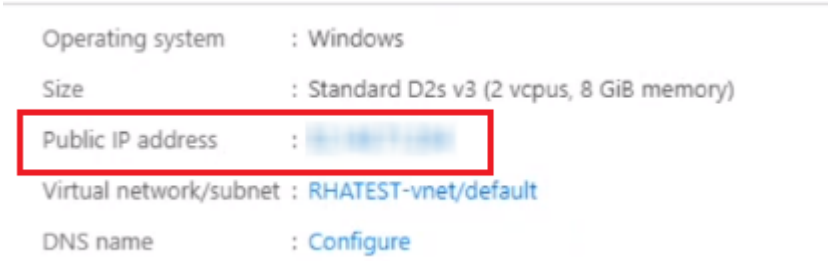


16. On the Virtual machines page, select the virtual machine.

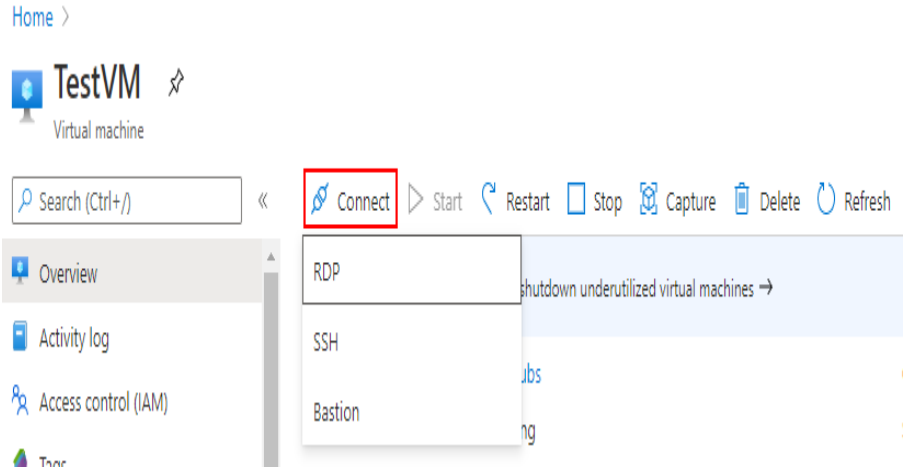


The overview page for your virtual machine opens.

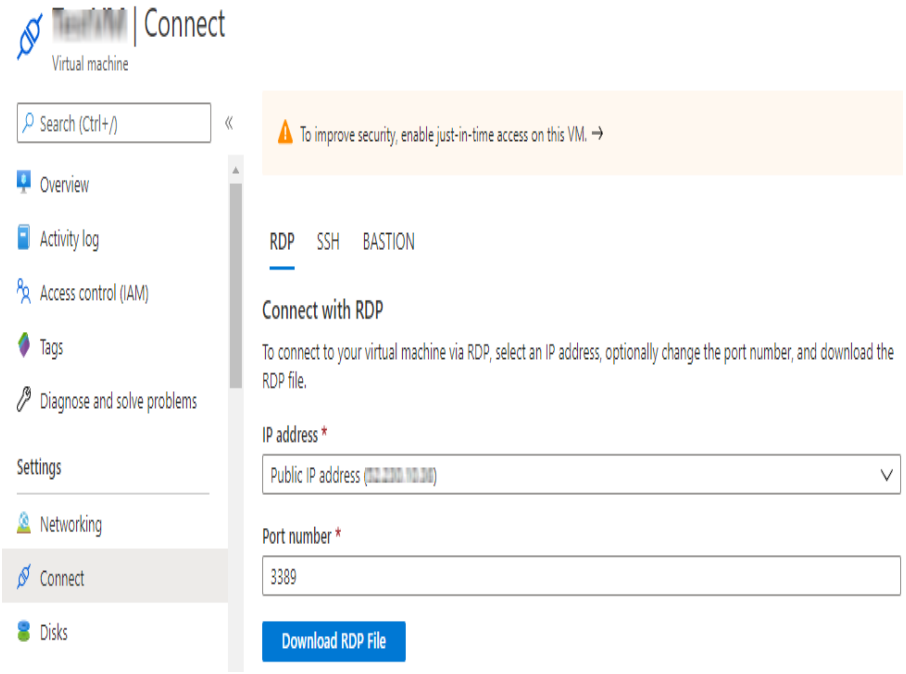
17. On the overview page, select the public IP address and copy it to the clipboard.



18. On the overview page, to connect to the virtual machine, do the following:
    a. Click the **Connect** button, and then select **RDP** option from the drop-down list.

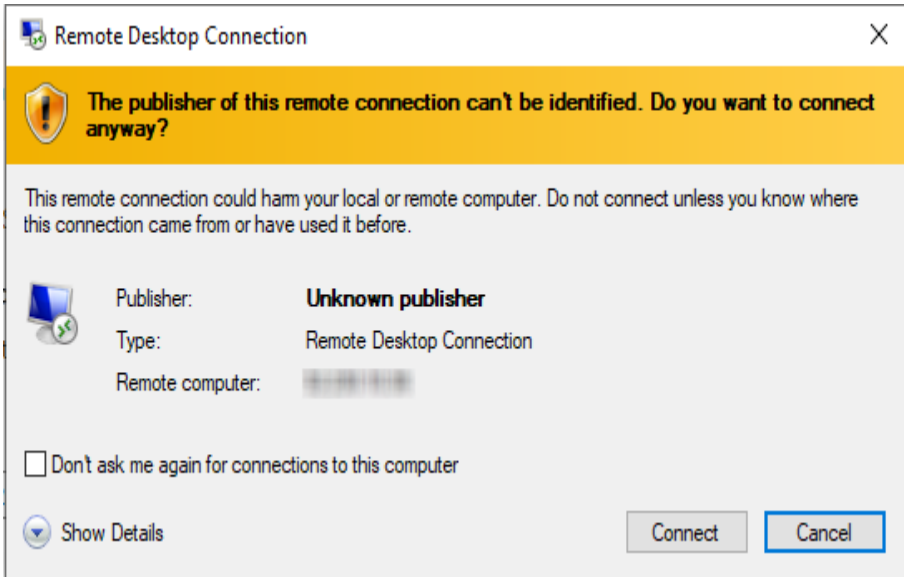


b. On the Connect page, click the **Download RDP file**.



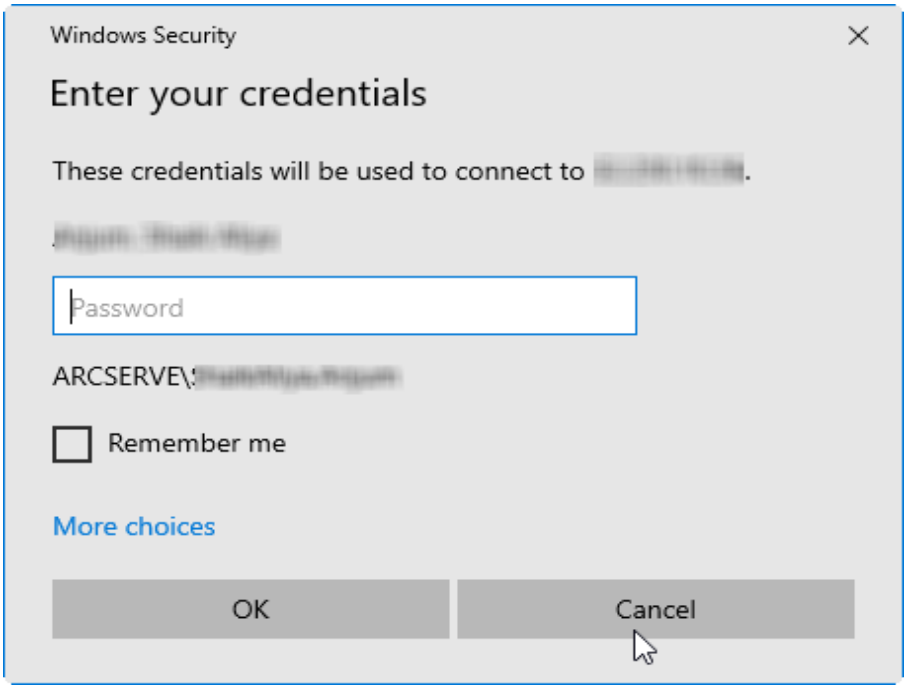
c. Click the downloaded file.

The Remote Desktop Connection page appears.



d. Click **Connect**.

The Enter your credentials screen appears.



e. Enter the password, and then click **OK**.

The virtual machine is now created on Microsoft Azure.

Install Engine on Replica

To install Engine on Replica server, see Installing Engine.

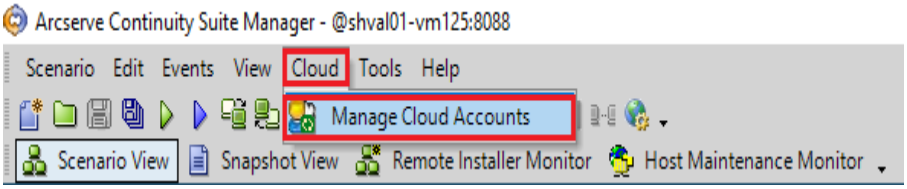
Create Full System Scenario for Microsoft Azure

Arcserve Live Migration supports both Windows and Linux for Full System scenario. If the source server is Windows, then the Virtual Appliance (VA) must be Windows. If the source server is Linux, then the VA must be Linux as well.

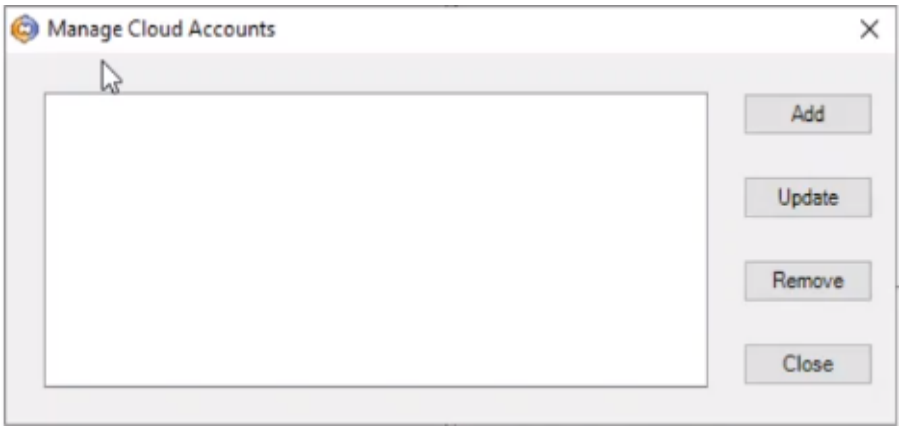
Before you create a scenario, add Azure Cloud Account in Continuity Suite Manager. For more information see, Configure Azure Cloud.

To add an Azure Cloud Account in Continuity Suite Manager, follow these steps:

1. On the Continuity Suite Manager, navigate to **Cloud** > **Manage Cloud Accounts**.

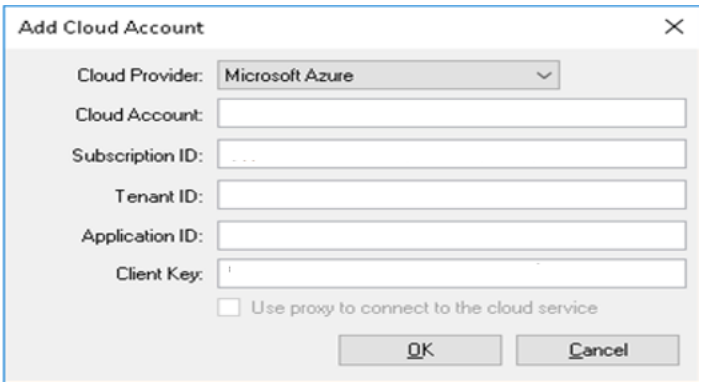


2. On the Manage Cloud Accounts screen, click **Add**.



3. On the Add Cloud Account screen, enter the following details in the required fields, and then click **OK**:
   - Cloud Account - Provide the cloud account, which is a user name you have defined.
   - Subscription ID - Provide the Subscription ID.
   - Tenant ID - Provide the Tenant ID.
   - Application ID - Provide the Application ID.
   - Client Key - Provide the Client Key.

Note: For more information about how to configure the Azure account details, see Configure Microsoft Azure.



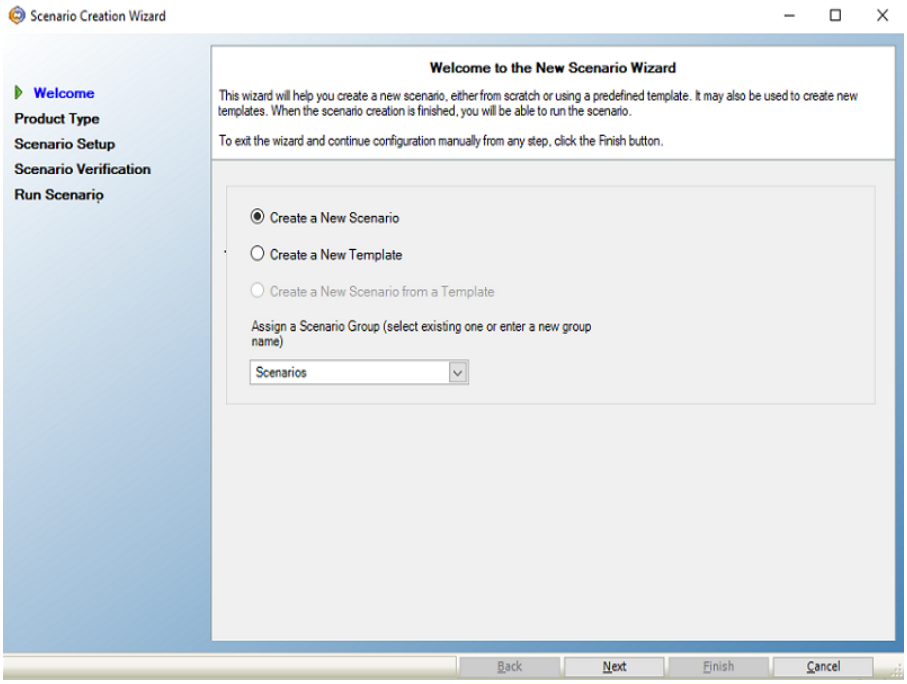
The Azure account for Live Migration is now added.

Creating Full System Scenario for Microsoft Azure

This section provides instructions on how to create full system scenario for Microsoft Azure. Before you begin, make sure to register and create an account in Azure.

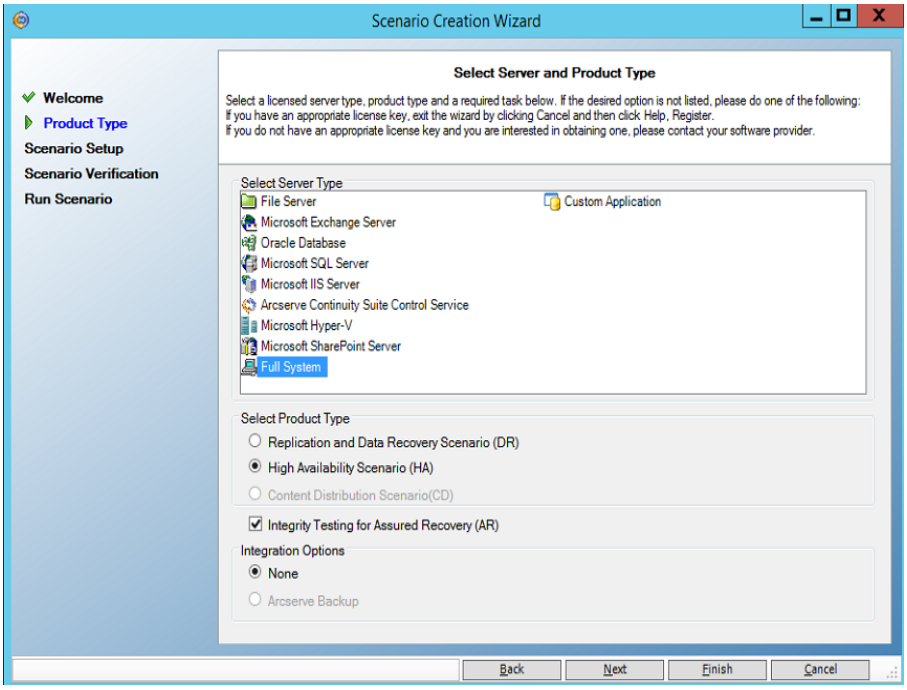
Follow these steps:

1. Open the Arcserve Continuity Suite Manager, navigate to **Scenario**>**New** or click the **New Scenario** button to launch the wizard.
2. On the Welcome to the New Scenario Wizard screen, select **Create a New Scenario**, select a Scenario Group from the list, and then click **Next**.

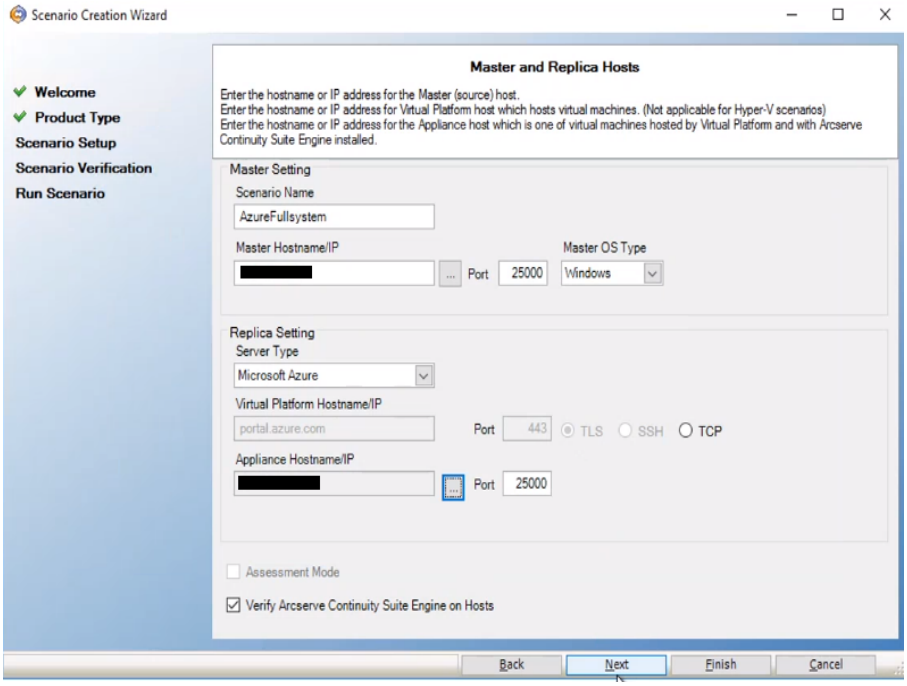


3. On the Select Server and Product Type screen, select Full System, High Availability Scenario (HA), and then click **Next**.

   Note: To perform Assured Recovery testing, select the **Integrity Testing for Assured Recovery (AR)** check box.



4. On the Master and Replica Hosts screen, do the following, and then click **Next**:

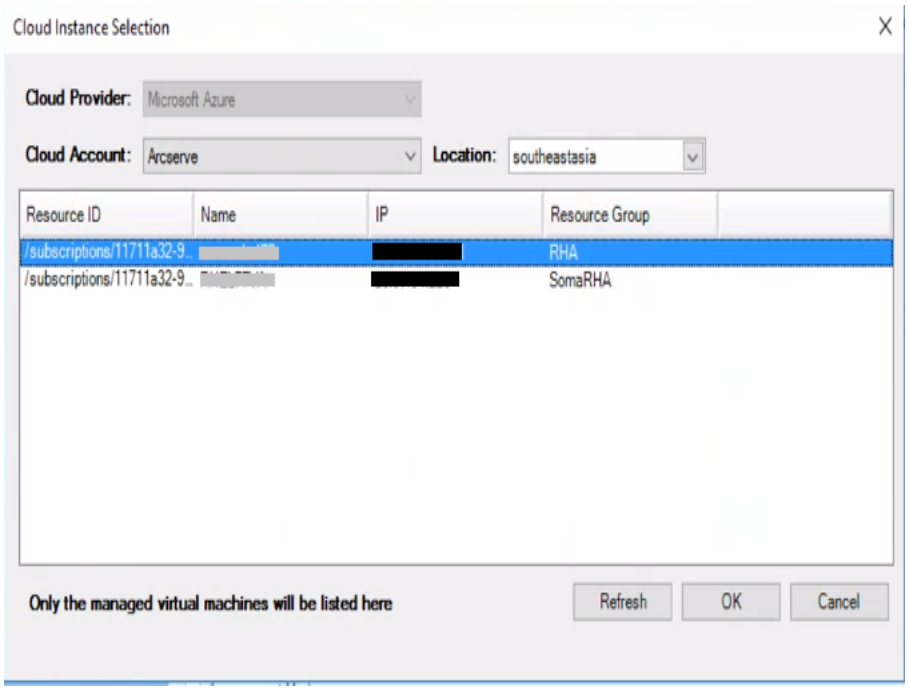


- Scenario Name - Enter a Scenario Name. The default value is the scenario type, for example, Full System.
- Master Hostname/IP - Enter the IP address of a physical machine you want to protect.
- Master OS Type - Select Windows as the Master OS Type.

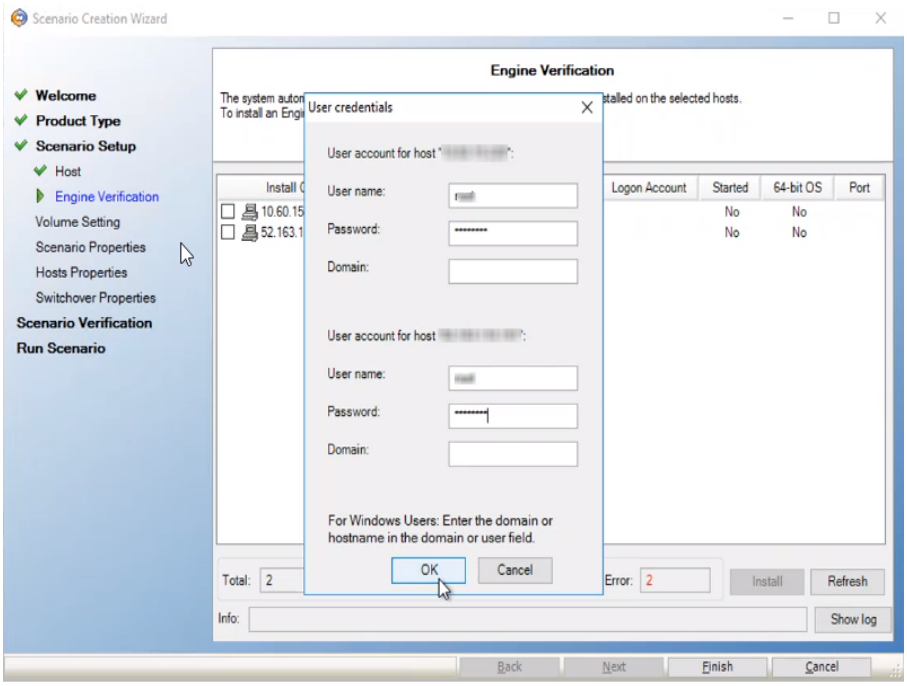
- Server Type - Select Microsoft Azure as the Replica server.
- Appliance Hostname/IP and Port - Browse the Appliance Hostname/IP to select the Replica server.

  Note: Select the **Verify Arcserve Continuity Suite Engine on Hosts** check box to verify the connectivity between Master and Replica. It verifies that the engines are installed on the Master. To skip verification, clear the check box.

  On the Cloud Instance Selection dialog, from the Location drop-down list, select the location. The list refreshes to display the relevant Azure instances. From the list, select the Azure instance you had created, and then click **OK**.

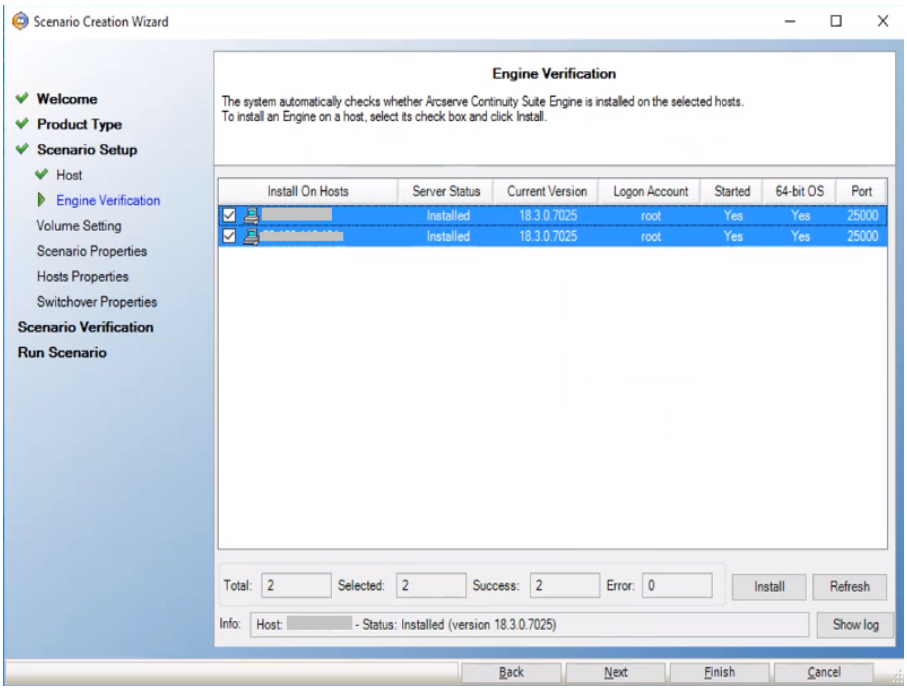


5. On the Engine Verification screen, the User credentials screen appears. Enter the user name and password, and then click **OK**.

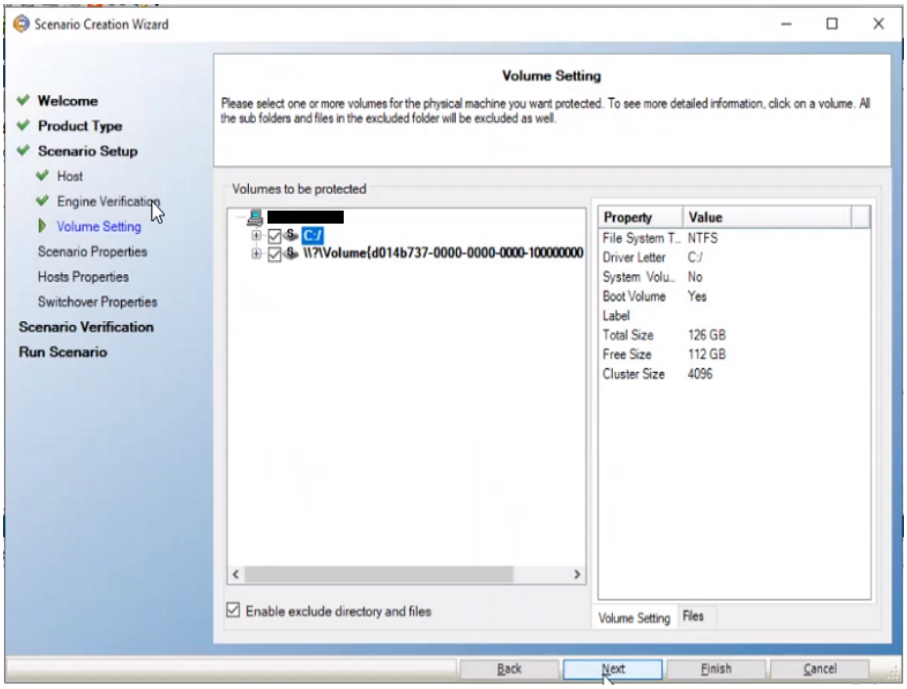


Wait for Engine verification to complete, and then click **Next**.

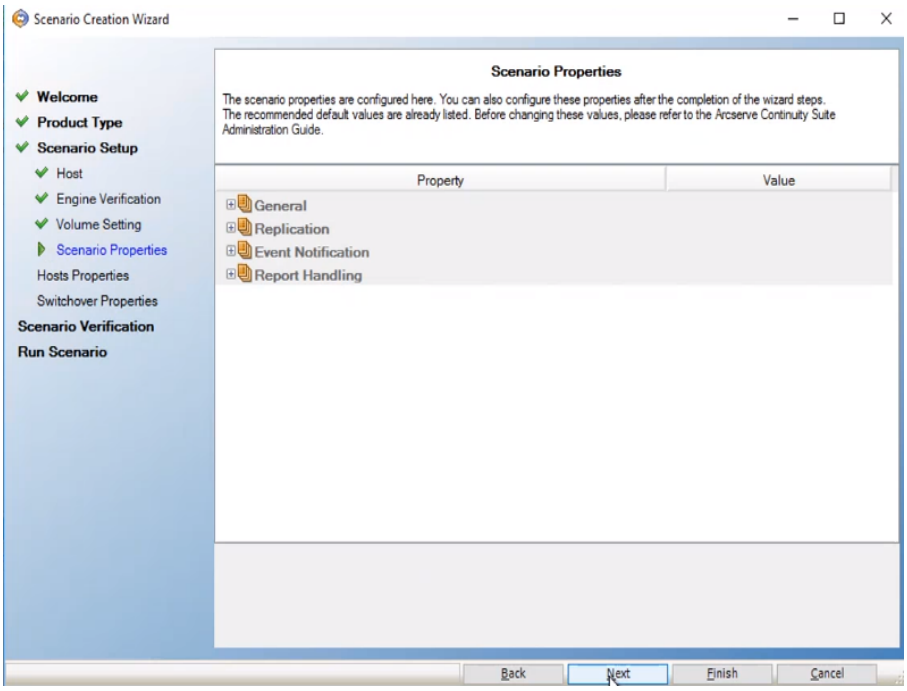
Note: If an error occurs, click **Install**. A confirmation message appears asking if the Engine can be upgraded on one or both servers; click **Yes**, and then click **Next**.



6. On the Volume Setting screen, select one or more volumes for the physical machine you want to protect, and then click **Next**.

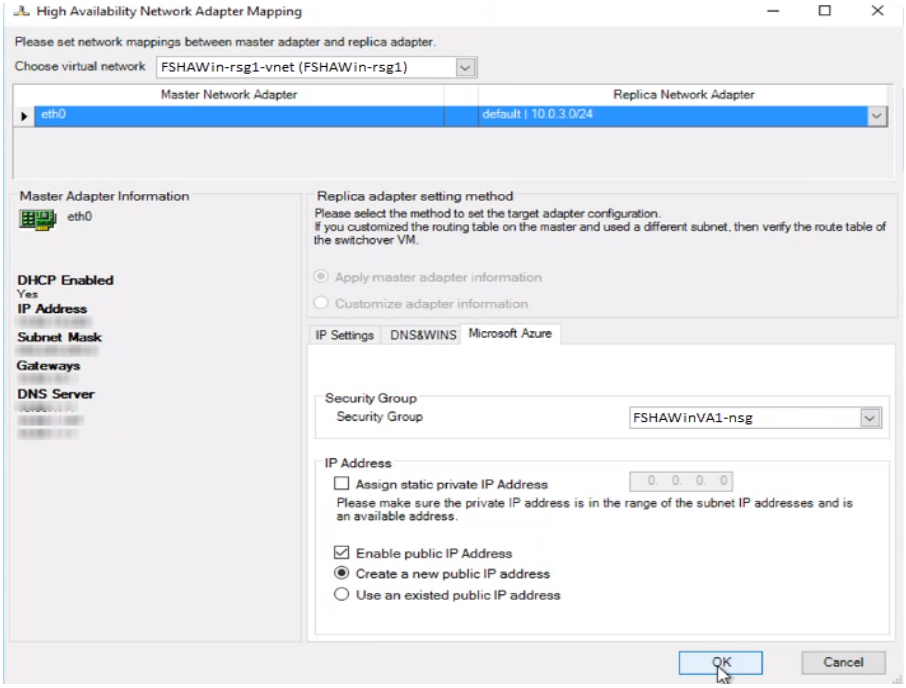


7. On the Scenario Properties screen, click **Next**.



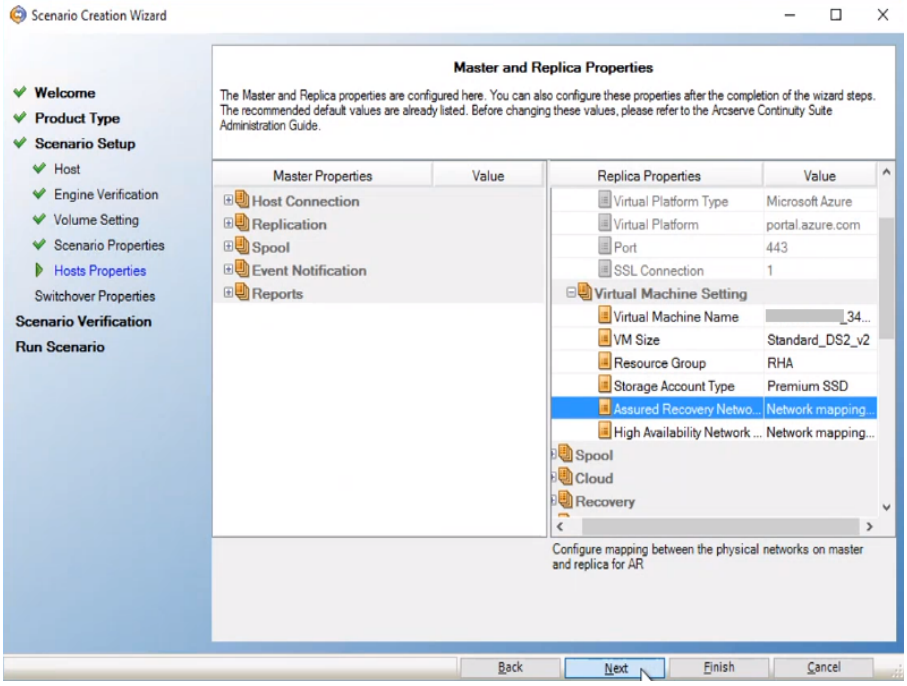
8. On the High Availability Network Adapter Mapping dialog, enter the following details, and then click **OK**:
   - Choose virtual network - Select virtual network from the drop-down list.
   - Replica Network Adapter - Select the Replica network adapter from the drop-down list.

- Security Group - Select the required security group from the drop-down list.
- IP Address - Select one of the following:
  - Assign static private IP Address
  - Enable public IP address
    - If you want to create a new public IP address, enable the **Create a new public IP address** option.
    - If you want to connect to the virtual machine from outside your network, enable the **Use an existed public IP address** option.

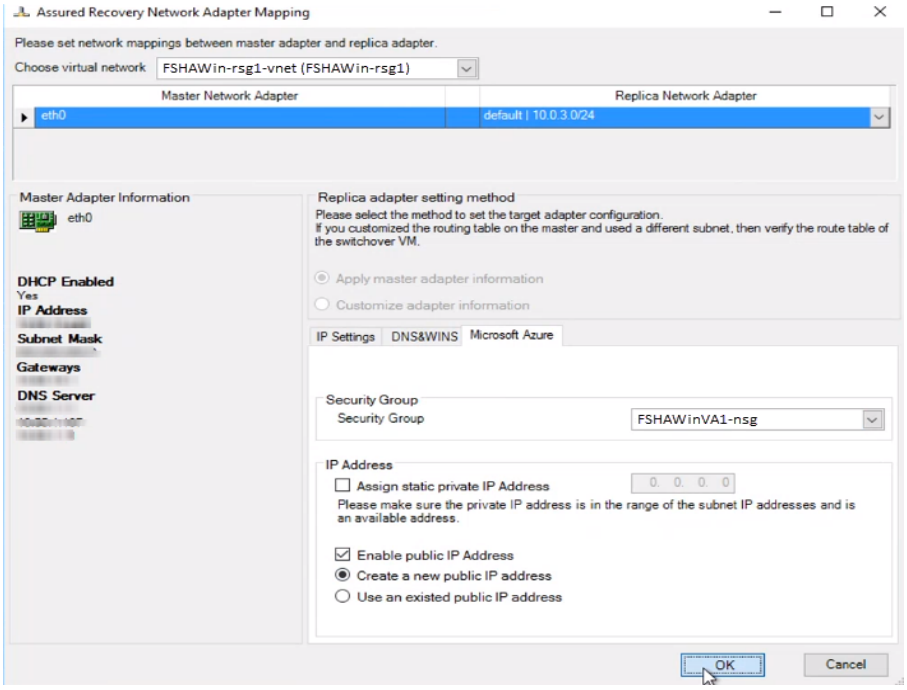


9. On the Master and Replica Properties screen, navigate to **Virtual Machine** -> **Virtual Machine Setting**, select **Assured Recovery Network**, and then click **Next**.

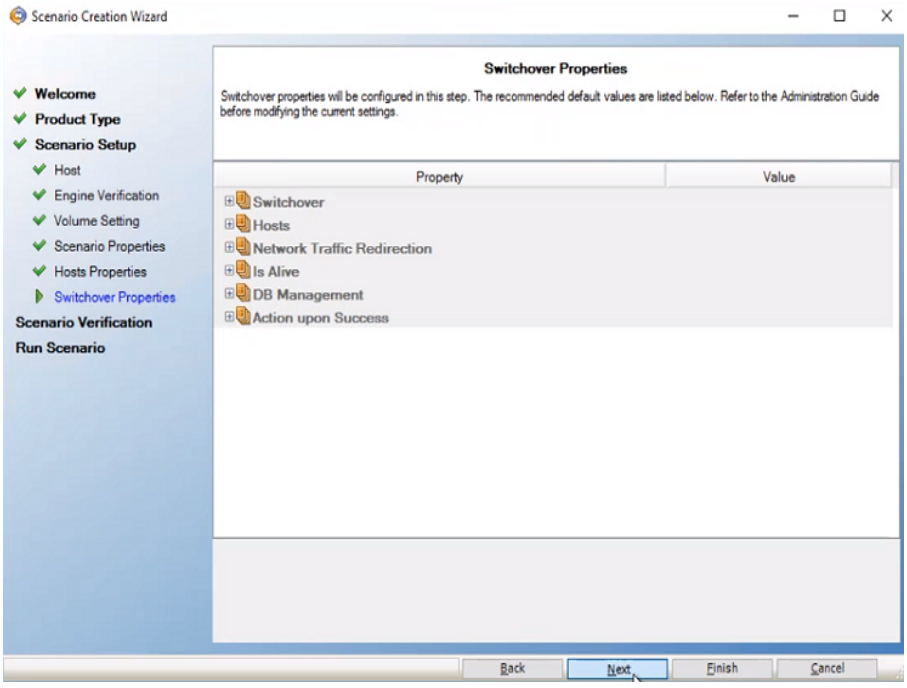
   Note: The **Assured Recovery Network** option displays only If you have enabled the **Integrity Testing for Assured Recovery (AR)** option on the Select Server and Product Type screen.



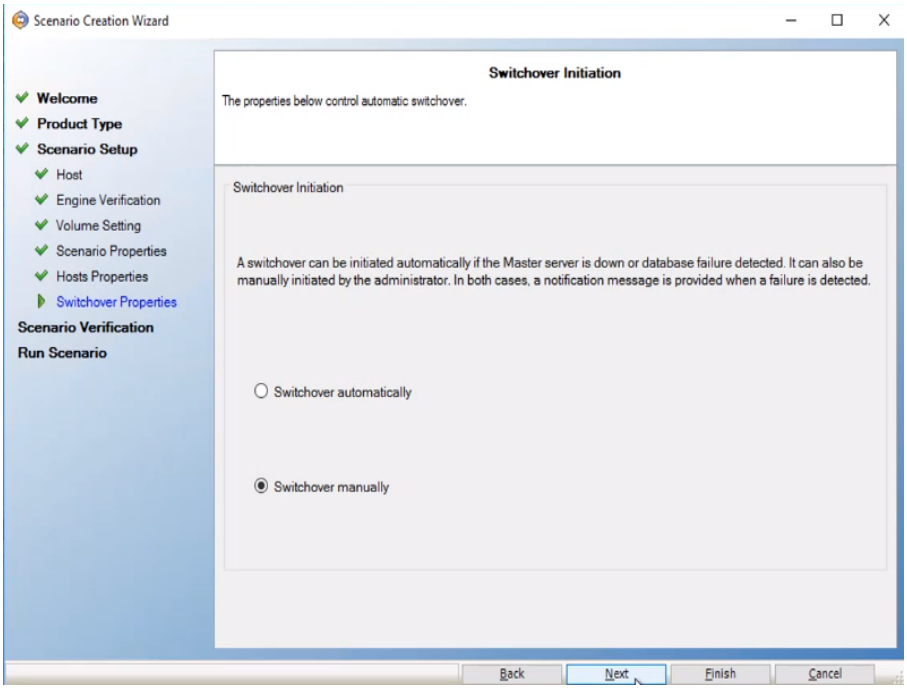
10. On the Assured Recovery Network Adapter Mapping dialog, enter the following details, and then click **OK**:
    - Choose virtual network - Select virtual network from the drop-down list.
    - Replica Network Adapter - Select the Replica network adapter from the drop-down list.
    - Security Group - Select the required security group from the drop-down list.
    - IP Address - Select one of the following:
        - Assign static private IP Address
        - Enable public IP address
            - If you want to create a new public IP address, enable the **Create a new public IP address** option.
            - If you want to connect to the virtual machine from outside your network, enable the **Use an existed public IP address** option.



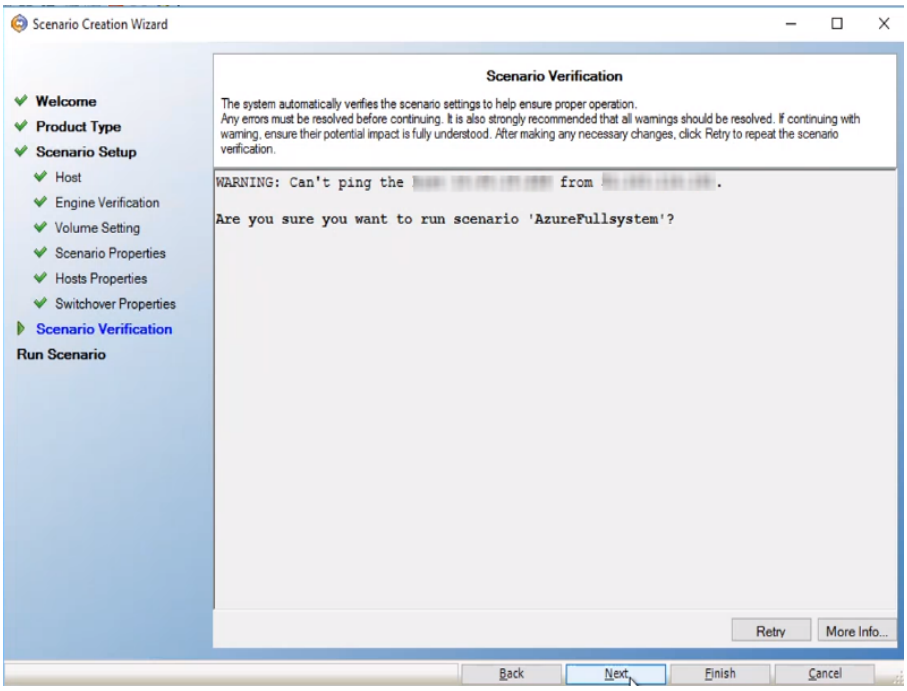
11. On the Switchover Properties screen, accept the default values or modify the values, and then click **Next**.



12. On the Switchover Initiation screen, specify if you want the switchover to start automatically (Switchover automatically) or manually (Switchover manually), and then click **Next**.



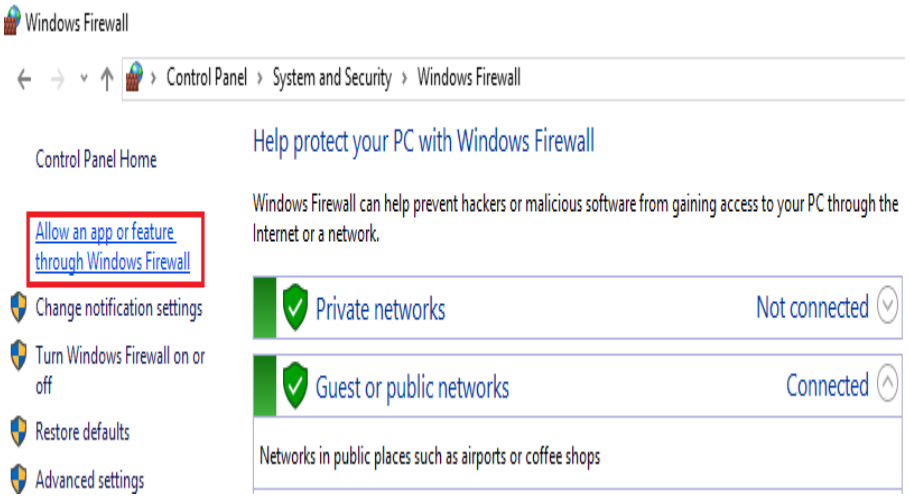
13. On the Scenario Verification screen, click **Next**.



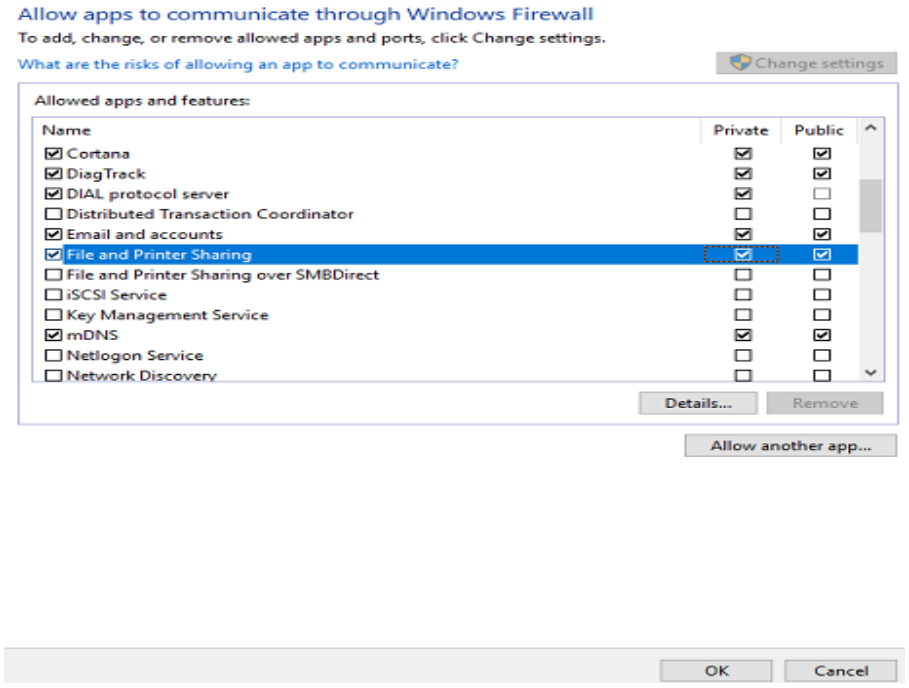
If the Master and Replica servers fail to ping each other, do the firewall and NAT settings.

- To do the firewall settings on both the Master server and the Azure VM, follow these steps:

1. Navigate to **Control Panel** > **System & Security** > **Windows Firewall** > **Allow an app or feature through Windows Firewall**.



2. On the Allow apps to communicate through Windows Firewall page, select the **File and Printer Sharing** check box, enable the **Private** and **Public** options, and then click **OK**.



- To do the NAT settings on the Master server, do the following:

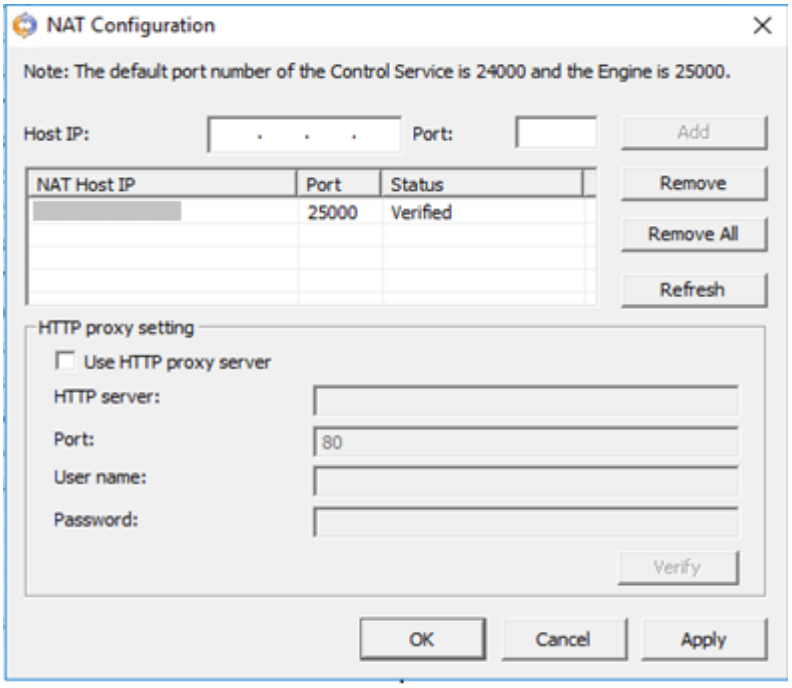
  1. Open the natutilgui from the engine installation directory.

     Note: The default installation directory is: C:\Program Files\Arcserve\RHA\Engine.

2. On the NAT Configuration dialog, do the following, and then click **Add**:

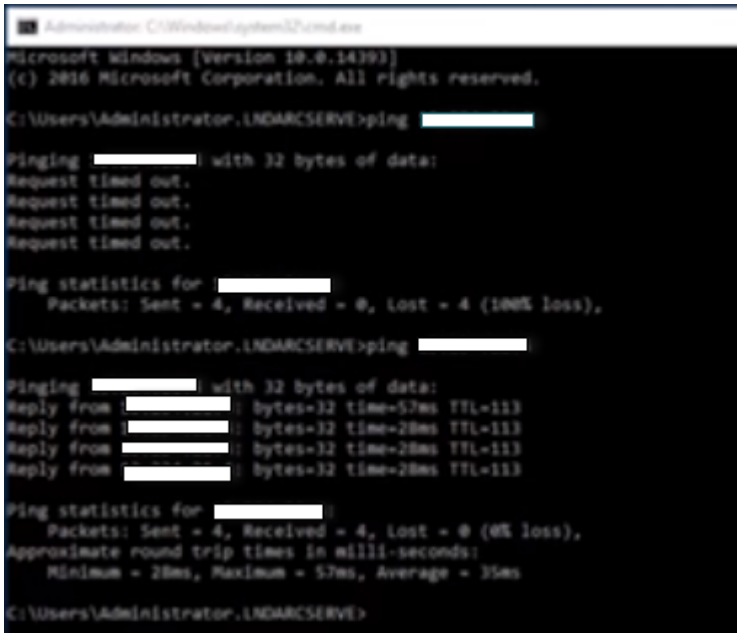
   Host IP: Type the Azure VM IP address.

   Port: Enter the port value as 25000.

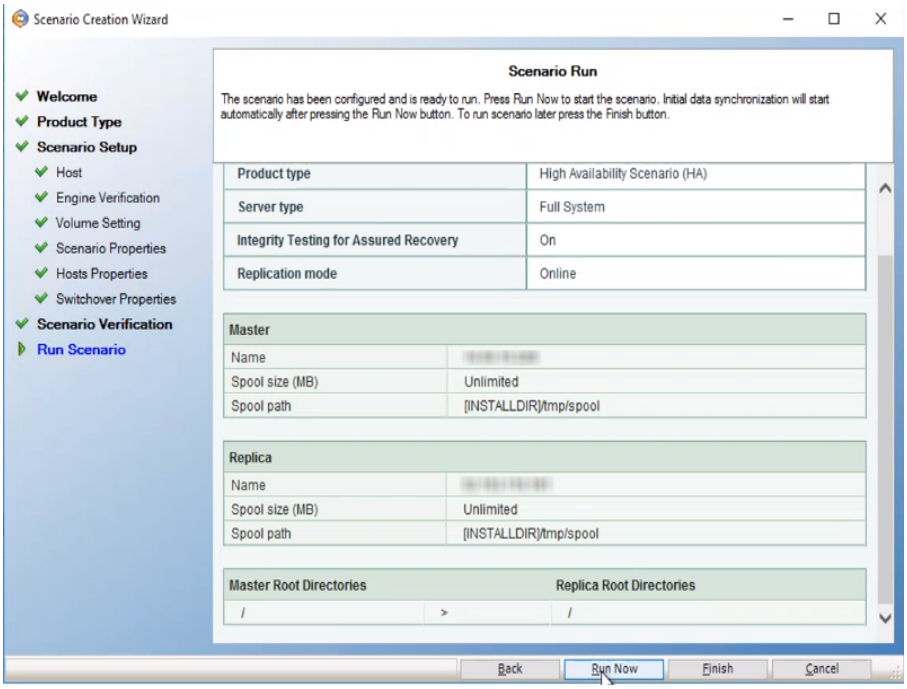


3. Click **Apply**, and then click **OK**.

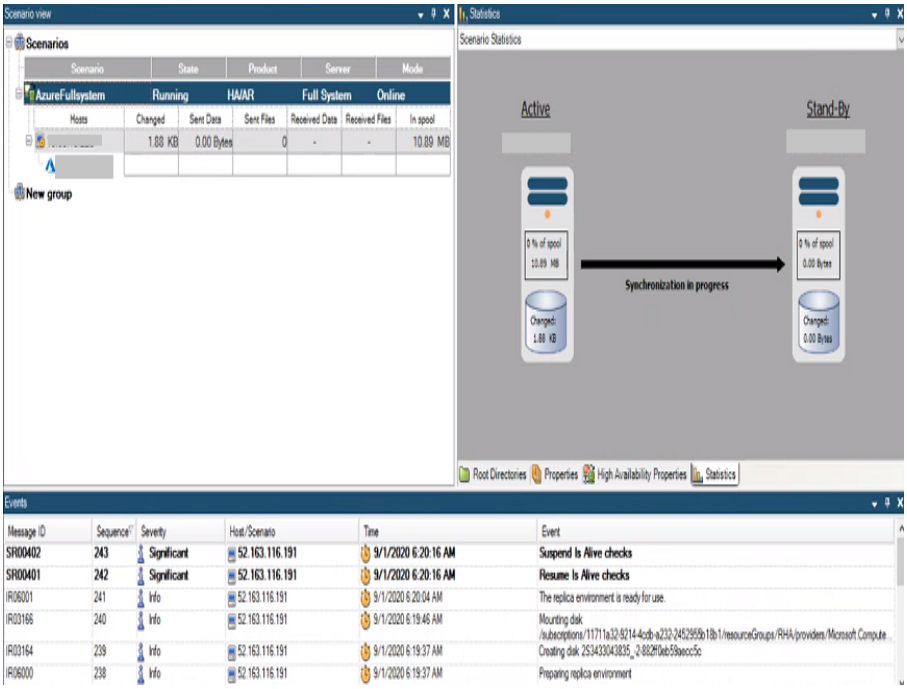
Now, the Master server can communicate with Replica server.



14. On the Scenario Run screen, to start synchronization immediately and activate the scenario, click **Run Now**. To save and run the scenario later, click **Finish**.



The synchronization between Master and Replica servers starts. Wait for synchronization to complete.



Perform Assured Recovery Testing

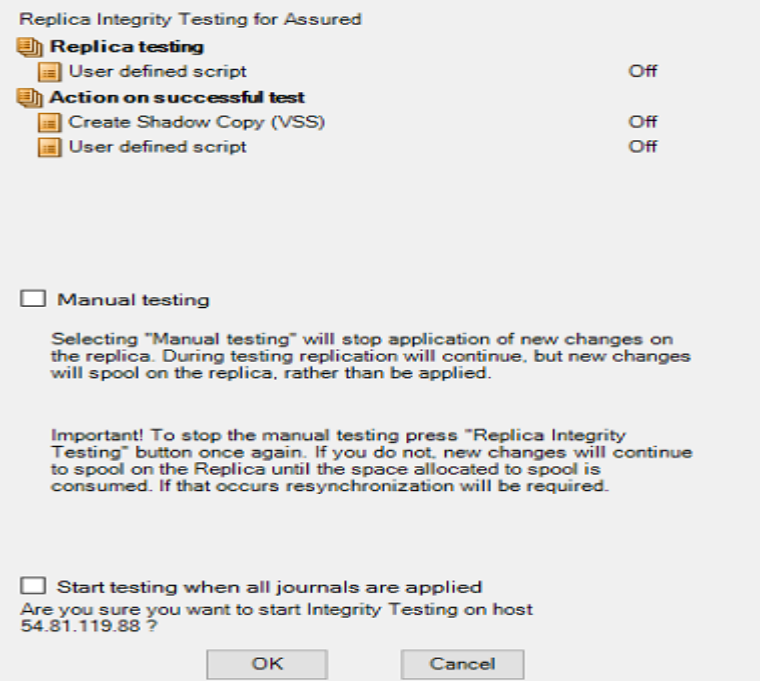
Note: Perform the Assured Recovery test only if you have enabled the **Integrity Testing for Assured Recovery (AR)** option on the Select Server and Product Type screen.

You can fully automate the Assured Recovery tests and schedule these tests as often as needed. On completion, an alert is sent to the appropriate personnel with the test status. You can also trigger additional actions such as taking a VSS snapshot of the data or running a backup. Alternatively, you can perform AR testing in a non-scheduled mode, and initiate the tests automatically or manually.

To perform AR test automatically, follow these steps:

1. On the Arcserve Continuity Suite Manager, verify that the AR scenario is running.
2. On the Standard toolbar, click the **Replica Integrity Testing** button, or right-click the Replica and select **Replica Integrity Testing** from the shortcut menu.

   The Replica Integrity Testing for Assured dialog opens.

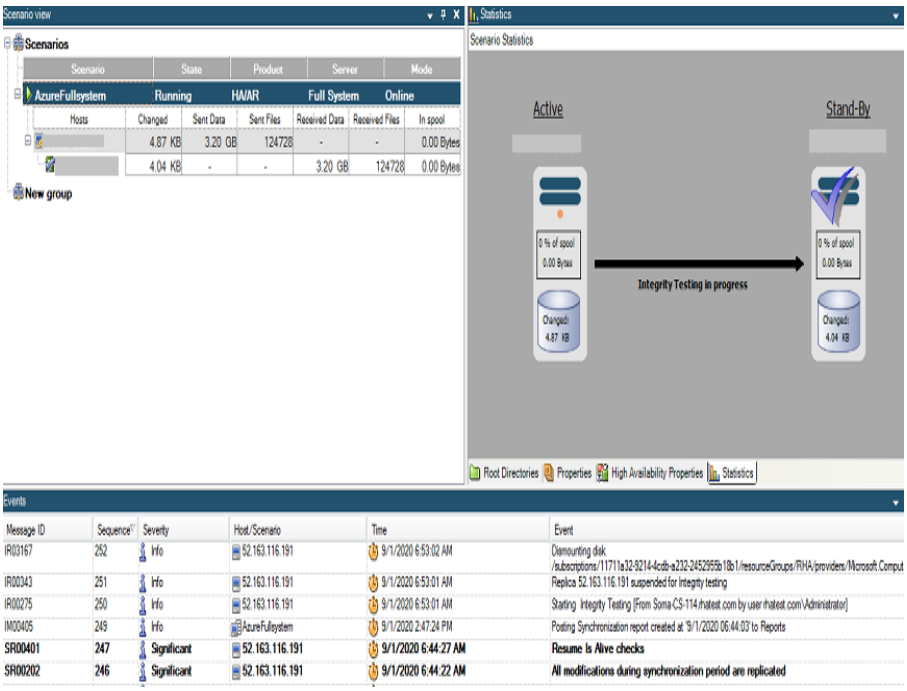


3. To start automatic AR test using the existing configuration, click **OK**.

   Notes:

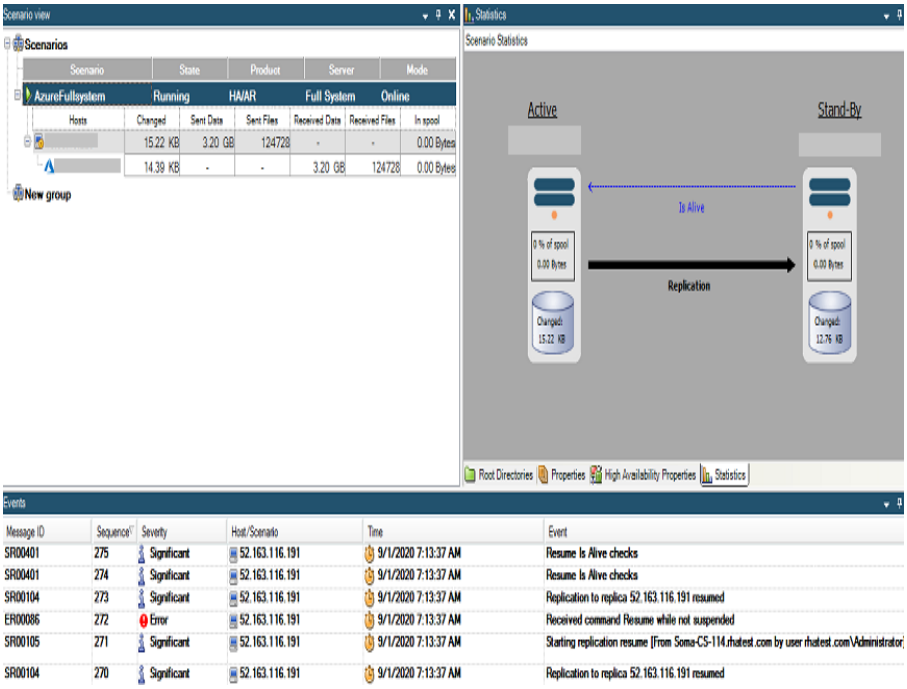
- To start the AR test manually, select the **Manual testing** checkbox, and then click **OK**.
- To change the test configuration before running the test, click **Cancel**. For more information, see Configure Assured Recovery Properties.
- Before the test begins to run, Arcserve Live Migration verifies that no synchronization, AR test or replication suspension tasks are in progress on any of the hosts that participate in the current scenario.

After the verification completes, the AR test begins.



The steps of the test are displayed as messages in the Event pane.

After the test is finished, the Replica is automatically restored to the same state it was when the replication was suspended. The changes that were accumulated in the spool gets applied, and the replication resumes.



By default, after the AR test is performed, an Assured Recovery Report is generated.

Notes:

- If the Assured Recovery Report is not generated, on the Replica Properties list, under the Reports group, check the value of the Generate Assured Recovery Report property.
- To view the report, see View a Report.

All the tasks that were performed during the AR test are listed in the AR Report, along with their activation time and status.

Perform Cut off/Switchover

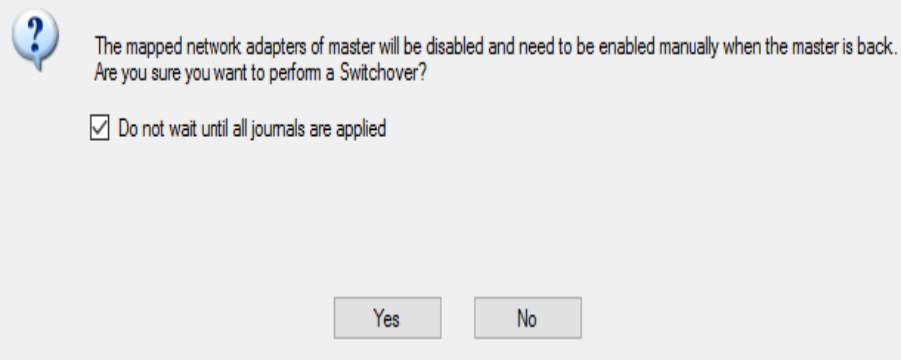
Switchover (or failover) is the process of changing roles between the Master and Replica, that is, making the Master server the standby server, and the Replica server the active server.

Switchover can be triggered automatically by Arcserve Live Migration when it detects that the Master is unavailable (failover). Alternatively, Arcserve Live Migration can simply alert you to the problem, and then you can manually initiate switchover from the Manager.

To perform switchover, follow these steps:

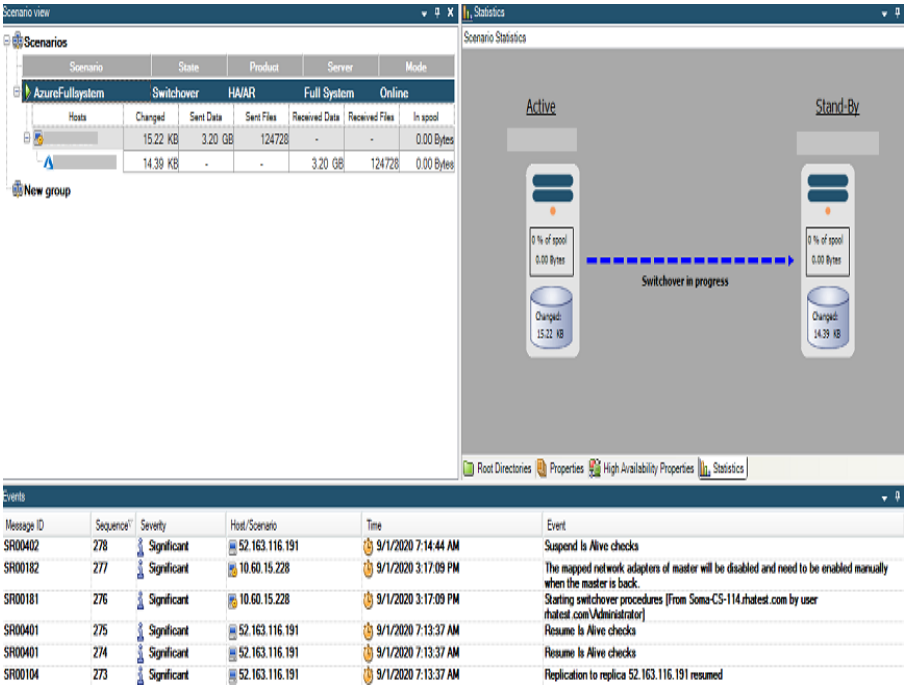
1. Open the Manager and then select the required scenario from the Scenario pane. Verify if it is running.
2. On the standard toolbar, click the **Perform Switchover** button, or select the Perform Switchover option from the **Tools** menu.

   A confirmation message appears.



3. [Optional] Select the **Do not wait until all journals are applied** check box to immediately perform switchover even before all journals are applied. If you do not select this check box, the switchover process gets initiated only after all journals are applied.
4. Click **Yes** on the confirmation message. This procedure initiates a switchover from the Master server to the Replica server.

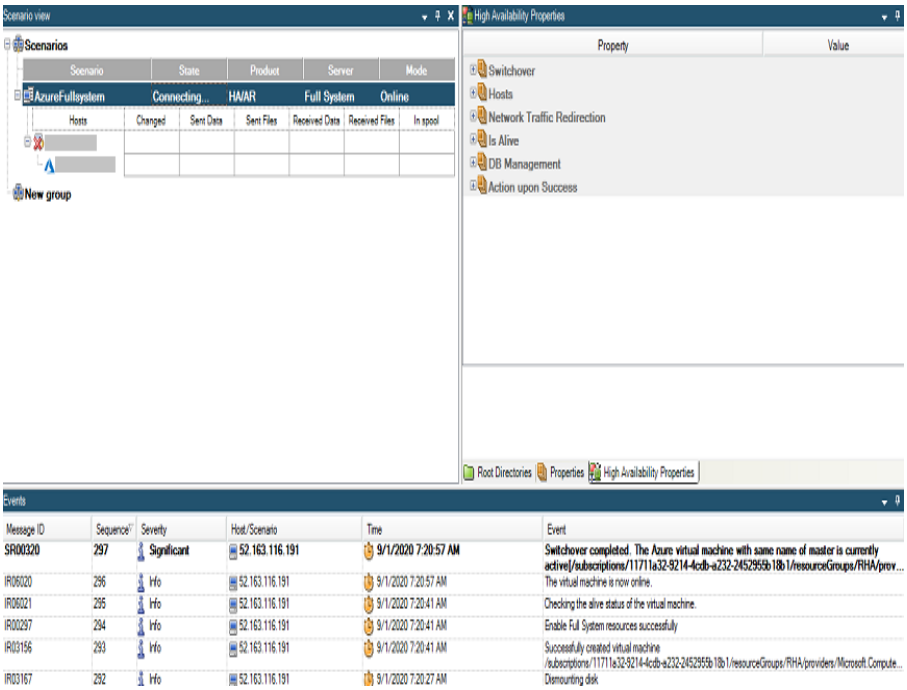
   During switchover, the Event pane gives detailed information about the switchover process.



After the switchover is complete, the scenario gets stopped.

Note: The only case in which the scenario may continue to run after switchover is when **automatic reverse replication** is defined as **Start automatically**.

When the switchover is completed, the Event pane displays the *Switchover completed* message.



Now, the original Master becomes the Replica, and the original Replica becomes the Master.